KANTON AARGAU

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon 062 835 12 40, Fax 062 835 12 50
regierungsrat@ag.ch
www.ag.ch/regierungsrat

A-Post Plus
Bundesamt für Justiz
Bundesrain 20
3003 Bern

22. September 2021

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassung

Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Juni 2021 wurden die Kantonsregierungen eingeladen, zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellung zu nehmen. Der Regierungsrat des Kantons Aargau dankt Ihnen für diese Möglichkeit und äussert sich wie folgt:

1. Allgemeines

Das revidierte Bundesgesetz über den Datenschutz (revDSG) vom 25. September 2020 beinhaltet zahlreiche Delegationsnormen, auf die sich der vorliegende E-VDSG stützt (siehe Ingress E-VDSG). Zudem konkretisiert der E-VDSG verschiedene Bestimmungen des revDSG. Insgesamt entsteht der Eindruck einer Verordnung, die (zu) wenig Klarheit für die Umsetzung durch die Verantwortlichen schafft. Einerseits liegt es darin, dass überholte Begriffe und Bestimmungen der bisherigen Verordnung einfach übernommen werden. Andererseits bringen die neuen Bestimmungen nicht die notwendige Detaillierung für die Umsetzung des an sich schon komplexen revDSG. Die Verantwortlichen – private Personen wie auch Bundesorgane – werden Mühe haben, verschiedene dieser Bestimmungen angemessen umzusetzen. Das Konzept der E-VDSG und einzelne Bestimmungen sollten deshalb im Hinblick auf eine wirkungsvolle Umsetzung des Datenschutzes grundsätzlich überprüft werden.

2. Einzelne Bestimmungen

2.1 Art. 1–4 E-VDSG (Datensicherheit)

Die Art. 1–4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 revDSG). Dabei verlangt Art. 8 Abs. 3 revDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt.

Der E-VDSG verpasst es, diese Mindestanforderungen in einer Form zu konkretisieren, die auch in Bezug auf die strafbewehrte Unterlassung der Umsetzung der Mindestanforderungen (Art. 61 Abs. 1 Bst. c revDSG) objektive Tatbestandsmerkmale erkennen lassen würde. In Bezug auf die Datensicherheit ist in der Informationsbearbeitung heute ein Standard erreicht, der klar nach der Beurteilung des Schutzbedarfs und der Risiken die entsprechenden Sicherheitsmassnahmen vorschlägt und einteilt (Grundschutz, hoher Schutz, sehr hoher Schutz). Der Bund hat soeben mit der Verabschiedung

des Bundesgesetzes über die Informationssicherheit (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020 gezeigt, wie die heutigen Anforderungen auch gesetzestechnisch umgesetzt werden können. Der E-VDSG hält dagegen am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht, ohne aber Art. 8 revDSG für die Praxis zu konkretisieren. Der Abschnitt 1 (Datensicherheit) ist entsprechend konzeptionell zu überarbeiten.

2.2 Art. 1 E-VDSG

Art. 1 Abs. 1 E-VDSG schreibt eine Beurteilung der Angemessenheit von Massnahmen nach den Kriterien Zweck, Art, Umfang und Umstände der Datenbearbeitung, Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen, Stand der Technik und Implementierungskosten vor.

Hier wird im Wesentlichen Art. 32 der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union rezipiert, ohne aber das in diesem Artikel formulierte Ziel in den Vordergrund zu stellen: "ein dem Risiko angemessenes Schutzniveau zu gewährleisten". Mitunter bedeutet dies, dass die Schutzziele, der Schutzbedarf und die Risiken zuerst zu beurteilen sind.

Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt, wie dies auch die Erläuterungen erwähnen (Seite 15) und werden in Art. 2 E-VDSG ausführlich aufgezählt (siehe nachfolgend Art. 2 E-VDSG). Der Schutzbedarf ergibt sich aus der Art der Daten (Personendaten, besonders schützenswerte Personendaten) und der Datenbearbeitung selbst (zum Beispiel Profiling). Erst dann erfolgt die Risikobeurteilung, wie dies auch die Datenschutz-Folgenabschätzung vorsieht (Art. 22 revDSG). Die Kriterien "Zweck, Art, Umfang und Umstände der Datenbearbeitung" beziehen sich somit auf die Schutzbedarfsfeststellung (welche bereits eine erste grobe Einschätzung des möglichen Schadensausmasses enthält), die Kriterien "Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen" auf die Risikobeurteilung.

Wenn es um die Beurteilung der Angemessenheit der Massnahmen geht, sind die Kriterien "Stand der Technik und Implementierungskosten" einschlägig. Sie sagen aber nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche dem Risiko mit der nötigen Effektivität begegnet. Dies ist im erwähnten ISG so angelegt, aber auch in Art. 32 DSGVO, der hier zitiert wird (Erläuterungen, Seite 15). Art. 1 Abs. 1 E-VDSG ist deshalb konzeptionell grundsätzlich zu überarbeiten.

Art. 1 Abs. 2 E-VDSG verlangt, dass die *Massnahmen* über die gesamte Bearbeitungszeit in angemessenen Abständen zu überprüfen sind. Diese Formulierung greift zu kurz. In erster Linie ist die *Risikobeurteilung* laufend zu überprüfen, woraus sich die Massnahmen und deren Angemessenheit ergeben und somit die allfällige Anpassung von Massnahmen. Die Formulierung ist zu korrigieren.

2.3 Art. 2 E-VDSG

Die Aufzählung der Schutzziele wurde aus der geltenden Verordnung übernommen und mit Bestimmungen aus der DSGVO ergänzt. Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt und lassen sich in die in der Informatiksicherheit üblichen Schutzziele zusammenfassen: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit (so auch Erläuterungen, Seite 15). Es erscheint als angezeigt, dies entsprechend klar zum Ausdruck zu bringen (vgl. in diesem Sinne Art. 6 Abs. 2 ISG).

Die in Art. 2 aufgeführten Vorgaben stellen keine eigenständigen Schutzziele dar, sondern Anforderungen an die Massnahmen, welche zur Erreichung der Schutzziele zu treffen sind (so stellt etwa die Zugriffskontrolle kein Schutzziel dar, sondern eine Anforderung zur Gewährleistung der Vertraulichkeit im Rahmen des Verhältnismässigkeitsprinzips). Zudem ist der Einleitungssatz von Art. 2

E-VDSG missverständlich. Schutzziele sind Zielvorgaben. Die Massnahmen müssen angemessen sein in Bezug auf die in der Risikobeurteilung festgestellten Risiken und nicht in Bezug auf die Schutzziele.

2.4 Art. 3 E-VDSG

Art. 3 E-VDSG sieht insbesondere für Bundesorgane eine ausführliche Protokollierung der Datenbearbeitungen vor. Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und dann unter Umständen sanktioniert) werden kann. Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das mittels Protokollierung wirksam reduziert werden kann; dass ein irgendwie geartetes Risiko verbleibt, reicht nicht (es fehlt dann an der Verhältnismässigkeit der neuen Datenbearbeitung). Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen zu umfassende Berechtigungen implementiert werden müssen, weil nicht zum Vorherein bekannt ist, auf welche konkreten Daten der/die Berechtigte bei der Aufgabenerfüllung Zugang haben muss (zum Beispiel im Schengen-Informationssystem). Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert und stichprobenweise überprüft werden. Die Pflicht zur Protokollierung als kompensierende Massnahme ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert.

Für die Bundesorgane soll die Protokollierung für das Bearbeiten sämtlicher Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Hier wird weit über das Ziel hinausgeschossen. Die Protokollierung stellt selbst eine Beschaffung von Personendaten dar, die dem Grundsatz der Verhältnismässigkeit genügen muss. Zwar erlaubt Art. 57l Bst. b Ziff. 4 des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) die Aufzeichnung von Randdaten zum Nachvollzug des Zugriffs auf Datensammlungen, aber eben nur insoweit, als die Aufzeichnung verhältnismässig ist. Dass selbst bei einfachen Personendaten und selbst bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht klar über diese Anforderung hinaus. Die Bundesorgane sind deshalb in Absatz 1 aufzunehmen und auf Absatz 2 ist zu verzichten.

In Art. 3 Abs. 3 E-VDSG sollte vor "die Identität der Empfängerin oder des Empfängers" das Wort "gegebenenfalls" eingefügt werden, da es sich nicht bei jeder protokollierten Bearbeitung um eine Bekanntgabe handelt.

Gemäss Art. 3 Abs. 4 E-VDSG sind die Protokolle während zweier Jahre aufzubewahren und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei ist nicht in jedem Fall eine personenbezogene Auswertung erforderlich. Für die Bundesorgane legen die Art. 57m ff. RVOG und Art. 8 ff. der zugehörigen Ausführungs-verordnung fest, wie die Auswertungen erfolgen dürfen, wobei ggf. auch ein gestaffeltes Vorgehen angezeigt ist (vgl. BGE 143 II 443). Der letzte Satz ist deshalb im Sinne "dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden" zu ergänzen.

2.5 Art. 4 E-VDSG

Die Erstellung eines Bearbeitungsreglements wird für private Verantwortliche und deren Auftragsbearbeiter vorgesehen, die (1) umfangreich besonders schützenswerte Personendaten bearbeiten oder (2) ein Profiling mit hohem Risiko durchführen (Art. 4 Abs. 1 E-VDSG). Diese Eingrenzung erscheint willkürlich und deckt bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen ab. Hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG). Im Rahmen der Datenschutz-Folgenabschätzung

werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 revDSG), die Teil des Bearbeitungsreglements sein können.

Art. 4 Abs. 2 E-VDSG enthält Mindestangaben für das Datenbearbeitungsreglement. Auch hier wird kein Konnex zu den Standards in der Informatik gemacht, in dem auf diese verwiesen würde. Dann würde es genügen, auf die spezifischen datenschutzrechtlichen Vorgaben hinzuweisen (Bst. h, j).

Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater ist die Fachperson bei einem Verantwortlichen und ein Bearbeitungsreglement wird zusammen mit ihr/ihm erstellt und nicht "der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung" gestellt. Es gehört zu den Aufgaben der Datenschutzberaterin oder des Datenschutzberaters, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b revDSG). Zudem hat die Datenschutzberaterin oder der Datenschutzberater über die erforderlichen Fachkenntnisse zu verfügen (Art. 10 Abs. 3 Bst. c revDSG), weshalb die Formulierung, das Bearbeitungsreglement sei ihr oder ihm "in verständlicher Form" zur Verfügung zu stellen, offensichtlich eine Abwertung seiner Fachkompetenzen impliziert. Art. 4 Abs. 3 E-VDSG ist ersatzlos zu streichen.

2.6 Art. 5 E-VDSG

Grundsätzlich kann auf unsere Ausführungen zu Art. 4 E-VDSG verwiesen werden.

2.7 Art. 7 E-VDSG

Auch die Datenschutzberaterin oder der Datenschutzberater des Bundesorgans hat bei der Anwendung der Datenschutzvorschriften mitzuwirken (vgl. unten Art. 28 E-VDSG). Es widerspricht dem präventiven und risikoorientierten Ansatz des revDSG, wenn die Datenschutzberaterin oder der Datenschutzberater lediglich nachträglich über den Abschluss eines Outsourcingvertrags oder bei einer Funktionsübertragung informiert werden soll. Zu den Aufgaben einer Datenschutzberaterin oder eines Datenschutzberaters gehört die Involvierung in solche Geschäfte. Dies ist eine Kernaufgabe der Beraterin oder des Beraters ("Mitwirkung bei der Anwendung der Datenschutzvorschriften"). Die Datenschutzberaterin oder der Datenschutzberater ist rechtzeitig zu informieren, wie dies korrekterweise bei Datenbearbeitungsprojekten vorgesehen ist (Art. 31 E-VDSG). Art. 7 E-VDSG ist somit ersatzlos zu streichen.

2.8 Art. 8 E-VDSG

Bei den Formulierungen in Art. 8 E-VDSG fällt auf, dass der EDÖB konsultiert wird (formell), und die Beurteilungen von internationalen Organisationen oder ausländischen Behörden berücksichtigt werden können (materiell). Es ist klar zu formulieren, dass auch die Stellungnahmen des EDÖB materiell zu berücksichtigen sind, zumal sich die Erläuterungen hierzu nicht äussern (Erläuterungen, Seite 27).

2.9 Art. 9 Abs. 3 E-VDSG

Gemäss Art. 16 Abs. 2 Bst. b und c revDSG sind Datenschutzklauseln und spezifische Garantien dem EDÖB vorgängig mitzuteilen. Der Einleitungssatz von Art. 9 Abs. 3 E-VDSG suggeriert, dass es einen Sachverhalt geben könnte, in der auch die Nicht-Mitteilung zu einer rechtskonformen Bekanntgabe ins Ausland führen würde. Die Formulierung ist entsprechend anzupassen.

2.10 Art. 19 E-VDSG

Art. 24 Abs. 1 revDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 revDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 revDSG).

Art. 24 revDSG ist eine (bewusst) abweichende Bestimmung von Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO rezipiert. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen. Für die Mehrheit der Verantwortlichen ist dies aber nicht der Fall und Art. 19 E-VDSG bringt unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung "wenn möglich". Dies ist dem Institut der Meldepflicht wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde rasch informiert wird, allenfalls auch die betroffenen Personen, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden. Art. 24 revDSG braucht dementsprechend die in Art. 19 E-VDSG enthaltene Konkretisierung nicht.

2.11 Art. 20 E-VDSG

Art. 25 revDSG und Art. 26 revDSG regeln das Auskunftsrecht und dessen Einschränkungen ausführlich. Art. 20 E-VDSG bringt hierzu einige Konkretisierungen, die aber über das Notwendige hinausgehen.

Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 revDSG definiert. Daraus ergeben sich der Umfang und der Zweck der Auskunft. Dies misst sich nach objektiven Kriterien. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte. Art. 20 Abs. 3 E-VDSG ist ersatzlos zu streichen.

Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, "die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen". Dies ergibt sich bereits aus Art. 8 revDSG und den Bestimmungen des 1. Kapitels der E-VDSG. Diese Erwähnung ist in Art. 20 Abs. 4 E-VDSG zu streichen.

Art. 26 Abs. 4 revDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person. Art. 20 Abs. 5 E-VDSG ist ersatzlos zu streichen.

2.12 Art. 21 E-VDSG

Art. 21 Abs. 1 E-VDSG sieht vor, dass ein Verantwortlicher, der für die Behandlung des Begehrens nicht zuständig, dieses an den zuständigen Verantwortlichen weiterleitet. Dieser verwaltungsrechtliche Grundsatz gilt für die Bundesorgane auch ohne Erwähnung in diesem Zusammenhang. Im öffentlich-rechtlichen Bereich ergibt er sich aus dem hoheitlichen Verhältnis der Bürgerinnen und Bürger zum Staat. Im privatrechtlichen Verhältnis legen die Parteien ihre Rechte und Pflichten aber autonom fest. Die gleiche Auflage auch dem privatrechtlichen Verantwortlichen zu machen, ist unverhältnismässig. Sie führt zu einem Aufwand für den privatrechtlichen Verantwortlichen, den "zuständigen" Verantwortlichen ausfindig zu machen, ohne dass dadurch die Rechte der betroffenen Personen gestärkt würden. Art. 21 Abs. 1 2. Satz E-VDSG ist ersatzlos zu streichen.

2.13 Art. 24 E-VDSG

Art. 24 E-VDSG beinhaltet eine Konkretisierung von Art. 28 revDSG, indem er sich auf die sinngemässe Anwendung von Bestimmungen zum Auskunftsrecht verweist. Dies wird dem neuen Rechtsinstitut der "Datenportabilität" nicht gerecht und verkennt den durchaus vorhandenen Bedarf einer Konkretisierung der gesetzlichen Bestimmung (beispielsweise in Bezug auf die "gängigen elektronischen Formate" oder den "unverhältnismässigen Aufwand" bei der direkten Übertragung von einem Verantwortlichen zu einem anderen). Zudem wäre auch in Bezug auf die Ausnahmen der Kostenlosigkeit eine andere Regelung als beim Auskunftsrecht denkbar, da hier nicht der Persönlichkeitsschutz, sondern der wirtschaftliche Wert der Daten im Vordergrund steht. Art. 24 E-VDSG ist vollständig zu überarbeiten.

2.14 Art. 25 E-VDSG

Art. 25 E-VDSG hält fest, welche Aufgaben die Datenschutzberaterin oder der Datenschutzberater wahrnehmen muss. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 revDSG, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die er oder sie wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 revDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist missverständlich und zu korrigieren.

2.15 Art. 26 E-VDSG

In Anwendung von Art. 12 Abs. 5 revDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn (1) umfangreich besonders schützenswerte Personendaten bearbeitet werden oder (2) ein Profiling mit hohem Risiko durchgeführt wird. Wie bei Art. 4 Abs. 1 E-VDSG ist zu erwähnen, dass diese Eingrenzung bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG).

2.16 Art. 28 E-VDSG

Art. 28 E-VDSG legt die Aufgaben der Datenschutzberaterin oder Datenschutzberaters der Bundesorgane fest. In der Aufzählung von Art. 28 Abs. 2 E-VDSG fällt auf, dass die in Art. 10 Abs. 2 Bst. b revDSG festgelegte Aufgabe – die Mitwirkung bei der Anwendung der Datenschutzvorschriften – nicht erwähnt wird, sondern nur die Schulung und Beratung (Art. 10 Abs. 2 Bst. a revDSG). Wir gehen davon aus, dass es sich hier um ein Versehen handelt, ist doch die Mitwirkung bei der Anwendung der Datenschutzvorschriften eine Kernaufgabe von Datenschutzberaterinnen und Datenschutzberater. Diese Aufgabe ist in Art. 28 Abs. 2 E-VDSG zu ergänzen.

2.17 Art. 36 E-VDSG

Die Bestimmung ist überflüssig, weil sich diese Präzisierung bereits aus Art. 39 revDSG klar ergibt.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats

Stephan Attiger
Landammann

Joana Filippi
Staatsschreiberin

Kopie
- jonas.amstutz@bj.admin.ch

KANTON
APPENZELL INNERRHODEN

Landammann und Standeskommission

Sekretariat Ratskanzlei
Marktgasse 2
9050 Appenzell
Telefon +41 71 788 93 11
info@rk.ai.ch
www.ai.ch

Ratskanzlei, Marktgasse 2, 9050 Appenzell

Per E-Mail an
jonas.amstutz@bj.admin.ch

Appenzell, 30. September 2021

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Juni 2021 haben Sie uns die Vernehmlassungsunterlagen zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) zukommen lassen.

Die Standeskommission hat die Unterlagen geprüft. Sie ist mit der Vorlage grundsätzlich einverstanden, hat aber nachfolgende Anmerkungen:

1. Art. 1 bis 4 E-VDSG (Datensicherheit)

Die Art. 1 bis 4 E-VDSG sollen die Mindestanforderungen an die Datensicherheit nach Art. 8 nDSG konkretisieren, wobei die vorsätzliche Nichteinhaltung dieser Mindestsicherheitsanforderungen nach Art. 61 Abs. 1 lit c. nDSG mit Busse von bis zu Fr. 250'000.-- bestraft werden kann. In der vorliegenden Form sind die Mindestanforderungen für die Praxis und auch für die Strafverfolgungsbehörden zu wenig konkret und verständlich beschrieben. Der erste Abschnitt E-VDSG ist entsprechend zu überarbeiten.

2. Art. 20 E-VDSG (Modalitäten Auskunftsrecht)

Art. 20 Abs. 3 E-VDSG normiert, dass die Auskunft nach Art. 25 nDSG für die betroffene Person verständlich sein müsse. Dies ist selbstverständlich, daher ist Art. 20 Abs. 3 E-VDSG zu streichen. Art. 20 Abs. 4 E-VDSG ist überflüssig, da die Mindestanforderungen im ersten Abschnitt E-VDSG beschrieben sind. Demgemäss ist Art. 20 Abs. 4 E-VDSG ebenfalls zu streichen.

3. Art. 25 E-VDSG (Anforderungen und Aufgaben)

Art. 25 Abs. 1 E-VDSG konkretisiert Art. 10 Abs. 2 lit. b nDSG. Dies geht aber aus dem Verordnungstext nicht hervor, was entsprechend zu korrigieren ist.

4. Art. 36 E-VDSG

Art. 36 E-VDSG ist überflüssig, weil sich diese Präzisierung bereits aus Art. 39 nDSG klar ergibt. Daher ist der Artikel zu streichen.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Im Auftrage von Landammann und Standeskommission
Der Ratschreiber:

Markus Dörig

Zur Kenntnis an:
- Justiz-, Polizei- und Militärdepartement Appenzell I.Rh., Marktgasse 10d, 9050 Appenzell
- Ständerat Daniel Fässler, Weissbadstrasse 3a, 9050 Appenzell
- Nationalrat Thomas Rechsteiner (thomas.rechsteiner@parl.ch)

Appenzell Ausserrhoden

Regierungsrat

Regierungsgebäude
9102 Herisau
Tel. +41 71 353 61 11
Fax +41 71 353 68 64
kantonskanzlei@ar.ch
www.ar.ch

Regierungsrat, 9102 Herisau

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
per E-Mail: jonas.amstutz@bj.admin.ch
[PDF- und Wordversion]

Dr. iur. Roger Nobs
Ratschreiber
Tel. +41 71 353 63 51
roger.nobs@ar.ch

Herisau, 24. September 2021

Eidg. Vernehmlassung; Entwurf zur Totalrevision der Verordnung zum BG über den Datenschutz (VDSG); Stellungnahme des Regierungsrates von Appenzell Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Juni 2021 wurden die Kantonsregierungen vom Eidgenössischen Justiz- und Polizeidepartement (EJPD) eingeladen, zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) bis 14. Oktober 2021 Stellung zu nehmen.

Der Regierungsrat von Appenzell Ausserrhoden nimmt dazu wie folgt Stellung:

1. Allgemeines

Das revidierte Bundesgesetz über den Datenschutz vom 25. September 2020 (revDSG) beinhaltet zahlreiche Delegationsnormen, auf die sich der vorliegende E-VDSG stützt (siehe Ingress E-VDSG). Zudem konkretisiert der E-VDSG verschiedene Bestimmungen des revDSG. Insgesamt entsteht der Eindruck einer Verordnung, die (zu) wenig Klarheit für die Umsetzung durch die Verantwortlichen schafft. Einerseits liegt es darin, dass überholte Begriffe und Bestimmungen der bisherigen Verordnung einfach übernommen werden. Andererseits bringen die neuen Bestimmungen nicht die notwendige Detaillierung für die Umsetzung des an sich schon komplexen revDSG. Die Verantwortlichen – private Personen wie auch Bundesorgane – werden Mühe haben, verschiedene dieser Bestimmungen angemessen umzusetzen. Das Konzept der E-VDSG und einzelne Bestimmungen sollten deshalb im Hinblick auf eine wirkungsvolle Umsetzung des Datenschutzes grundsätzlich überprüft werden.

2. Einzelne Bestimmungen

a. Art. 1 bis 4 E-VDSG (Datensicherheit)

Die Art. 1 bis 4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 revDSG). Dabei verlangt Art. 8 Abs. 3 revDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt.
Der E-VDSG verpasst es, diese Mindestanforderungen in einer Form zu konkretisieren, die auch in Bezug auf die strafbewehrte Unterlassung der Umsetzung der Mindestanforderungen (Art. 61 Abs. 1 Bst. c revDSG) objektive Tatbestandsmerkmale erkennen lassen würde. In Bezug auf die Datensicherheit ist in der Informationsbearbeitung heute ein Standard erreicht, der klar nach der Beurteilung des Schutzbedarfs und der Risiken die

entsprechenden Sicherheitsmassnahmen vorschlägt und einteilt (Grundschutz, hoher Schutz, sehr hoher Schutz). Der Bund hat soeben mit der Verabschiedung des Bundesgesetzes über die Informationssicherheit (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020) gezeigt, wie die heutigen Anforderungen auch gesetzestechnisch umgesetzt werden können.
Der E-VDSG hält dagegen am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht, ohne aber Art. 8 revDSG für die Praxis zu konkretisieren.
Der Abschnitt 1 (Datensicherheit) ist konzeptionell grundsätzlich zu überarbeiten.

b. Art. 1 E-VDSG

Art. 1 Abs. 1 E-VDSG schreibt eine Beurteilung der Angemessenheit von Massnahmen nach den Kriterien Zweck, Art, Umfang und Umstände der Datenbearbeitung, Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen, Stand der Technik und Implementierungskosten vor. Hier wird im Wesentlichen Art. 32 DSGVO rezipiert, ohne aber das in diesem Artikel formulierte Ziel in den Vordergrund zu stellen: «ein dem Risiko angemessenes Schutzniveau zu gewährleisten». Mitunter bedeutet dies, dass die Schutzziele, der Schutzbedarf und die Risiken zuerst zu beurteilen sind.
Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt, wie dies auch die Erläuterungen erwähnen (S. 15) und werden in Art. 2 E-VDSG ausführlich aufgezählt (siehe nachfolgend Art. 2 E-VDSG). Der Schutzbedarf ergibt sich aus der Art der Daten (Personendaten, besonders schützenswerte Personendaten) und der Datenbearbeitung selbst (z.B. Profiling). Erst dann erfolgt die Risikobeurteilung, wie dies auch die Datenschutz-Folgenabschätzung vorsieht (Art. 22 revDSG).
Die Kriterien «Zweck, Art, Umfang und Umstände der Datenbearbeitung» beziehen sich somit auf die Schutzbedarfsfeststellung (welche bereits eine erste grobe Einschätzung des möglichen Schadensausmasses enthält), die Kriterien «Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen» auf die Risikobeurteilung.
Wenn es um die Beurteilung der Angemessenheit der Massnahmen geht, sind die Kriterien «Stand der Technik und Implementierungskosten» einschlägig. Sie sagen aber nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche dem Risiko mit der nötigen Effektivität begegnet. Dies ist im erwähnten ISG so angelegt, aber auch in Art. 32 DSGVO, der hier zitiert wird (Erläuterungen, S. 15).

Art. 1 Abs. 2 E-VDSG verlangt, dass die Massnahmen über die gesamte Bearbeitungszeit in angemessenen Abständen zu überprüfen sind. Diese Formulierung greift zu kurz. In erster Linie ist die Risikobeurteilung laufend zu überprüfen, woraus sich die Massnahmen und deren Angemessenheit ergeben und somit die allfällige Anpassung von Massnahmen.

c. Art. 2 E-VDSG

Die Aufzählung der Schutzziele mahnt an die Steinzeit der Informatik. Sie wurde aus der geltenden Verordnung übernommen und mit Bestimmungen aus der DSGVO ergänzt. Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt und lassen sich in die in der Informatiksicherheit üblichen Schutzziele zusammenfassen: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit (so auch Erläuterungen, S. 15).
Die Schutzziele sind in einer verständlichen Weise umzuformulieren. Beispiele finden sich in § des Informations- und Datenschutzgesetzes des Kantons Basel-Stadt oder § 7 des Informations- und Datenschutzgesetzes des Kantons Zürich. Zudem ist der Einleitungssatz von Art. 2 E-VDSG missverständlich. Schutzziele sind Zielvorgaben. Die Massnahmen müssen angemessen sein in Bezug auf die in der Risikobeurteilung festgestellten Risiken und nicht in Bezug auf die Schutzziele.

d. Art. 3 E-VDSG

Art. 3 E-VDSG sieht insbesondere für Bundesorgane eine ausführliche Protokollierung der Datenbearbeitungen vor.
Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und dann unter Umständen sanktioniert) werden kann. Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das mittels Protokollierung wirksam reduziert werden kann; dass ein irgendwie geartetes Risiko verbleibt, reicht nicht (es fehlt dann an der Verhältnismässigkeit der neuen Datenbearbeitung). Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen offene Berechtigungen implementiert werden müssen, weil nicht zum Vorherein bekannt ist, auf welche konkreten Daten der/die Berechtigte bei der Aufgabenerfüllung Zugang haben muss (z.B. im Schengen-Informationssystem). Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert und stichprobenweise überprüft werden. Die Pflicht zur Protokollierung ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert.

Für die Bundesorgane soll die Protokollierung für das Bearbeiten sämtlicher Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Hier wird weit über das Ziel hinausgeschossen. Die Protokollierung stellt selbst eine Beschaffung von Personendaten dar, die dem Grundsatz der Verhältnismässigkeit genügen muss. Zwar erlaubt Art. 57l Bst. b Ziff. 4 RVOG die Aufzeichnung von Randdaten zum Nachvollzug des Zugriffs auf Datensammlungen, aber eben nur insoweit, als die Aufzeichnung verhältnismässig ist. Dass selbst bei einfachen Personendaten und selbst bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht klar über diese Anforderung hinaus. Es ist nicht einzusehen, warum die Pflicht der Bundesorgane zur Protokollierung weitergehen soll als jene der privaten Verantwortlichen. Die Bundesorgane sind deshalb in Absatz 1 aufzunehmen und auf Absatz 2 ist zu verzichten.
In Art. 3 Abs. 3 E-VDSG sollte vor «die Identität der Empfängerin oder des Empfängers» das Wort «gegebenenfalls» eingefügt werden, da es sich nicht bei jeder protokollierten Bearbeitung um eine Bekanntgabe handelt.
Gemäss Art. 3 Abs. 4 E-VDSG sind die Protokolle während zweier Jahre aufzubewahren und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei ist nicht in jedem Fall eine personenbezogene Auswertung erforderlich. Für die Bundesorgane legen die Art. 57m ff. RVOG und Art. 8 ff. der zugehörigen Ausführungsverordnung fest, wie die Auswertungen erfolgen dürfen, wobei ggf. auch ein gestaffeltes Vorgehen angezeigt ist (vgl. BGE 143 II 443). Der letzte Satz ist deshalb im Sinne «dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden» zu ergänzen.

e. Art. 4 E-VDSG

Die Erstellung eines Bearbeitungsreglements wird für private Verantwortliche und deren Auftragsbearbeiter vorgesehen, die (1) umfangreich besonders schützenswerte Personendaten bearbeiten oder (2) ein Profiling mit hohem Risiko durchführen (Art. 4 Abs. 1 E-VDSG). Diese Eingrenzung erscheint willkürlich und deckt bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen ab. Es ist angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG). Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 revDSG), die Teil des Bearbeitungsreglements sein können.

Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater ist die Fachperson bei einem Verantwortlichen und ein Bearbeitungsreglement wird zusammen mit ihr/ihm erstellt und nicht «der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung» gestellt. Es gehört zu den Aufgaben der Datenschutzberaterin oder des Datenschutzberaters, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b revDSG). Zudem hat die Datenschutzberaterin oder der Datenschutzberater über die erforderlichen Fachkenntnisse zu verfügen (Art. 10 Abs. 3 Bst. c revDSG), weshalb die Formulierung, das Bearbeitungsreglement sei ihr oder ihm «in verständlicher Form» zur Verfügung zu stellen, offensichtlich eine Abwertung seiner Fachkompetenzen impliziert.
Art. 4 Abs. 3 E-VDSG ist ersatzlos zu streichen.

f. Art. 5 E-VDSG

Grundsätzlich kann auf unsere Ausführungen zu Art. 4 E-VDSG verwiesen werden.

g. Art. 19 E-VDSG

Art. 24 Abs. 1 revDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 revDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 revDSG).

Art. 24 revDSG ist eine (bewusst) abweichende Bestimmung von Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO rezipiert. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen. Für die Mehrheit der Verantwortlichen ist dies aber nicht der Fall und Art. 19 E-VDSG bringt unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde rasch informiert wird, allenfalls auch die betroffenen Personen, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden.

h. Art. 20 E-VDSG

Art. 25 revDSG und Art. 26 revDSG regeln das Auskunftsrecht und dessen Einschränkungen ausführlich. Art. 20 E-VDSG bringt hierzu einige Konkretisierungen, die aber über das Notwendige hinausgehen. Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 revDSG definiert. Daraus ergeben sich der Umfang und der Zweck der Auskunft. Dies misst sich nach objektiven Kriterien. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte.

Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen». Dies ergibt sich bereits aus Art. 8 revDSG und den Bestimmungen des 1. Kapitels der E-VDSG.

Art. 26 Abs. 4 revDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allen-

falls gerichtlich geltend zu machen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person.

i. Art. 21 E-VDSG

Art. 21 Abs. 1 E-VDSG sieht vor, dass ein Verantwortlicher, der für die Behandlung des Begehrens nicht zuständig, dieses an den zuständigen Verantwortlichen weiterleitet. Dieser verwaltungsrechtliche Grundsatz gilt für die Bundesorgane auch ohne Erwähnung in diesem Zusammenhang. Im öffentlich-rechtlichen Bereich ergibt er sich aus dem hoheitlichen Verhältnis der Bürgerinnen und Bürger zum Staat. Im privatrechtlichen Verhältnis legen die Parteien ihre Rechte und Pflichten aber autonom fest. Die gleiche Auflage auch dem privatrechtlichen Verantwortlichen zu machen, ist unverhältnismässig. Sie führt zu einem Aufwand für den privatrechtlichen Verantwortlichen, den «zuständigen» Verantwortlichen ausfindig zu machen, ohne dass dadurch die Rechte der betroffenen Personen gestärkt würden.

j. Art. 24 E-VDSG

Art. 24 E-VDSG beinhaltet eine Konkretisierung von Art. 28 revDSG, indem er sich auf die sinngemässe Anwendung von Bestimmungen zum Auskunftsrecht verweist. Dies wird dem neuen Rechtsinstitut der «Datenportabilität» nicht gerecht und verkennt den durchaus vorhandenen Bedarf einer Konkretisierung der gesetzlichen Bestimmung (beispielsweise in Bezug auf die «gängigen elektronischen Formate» oder den «unverhältnismässigen Aufwand» bei der direkten Übertragung von einem Verantwortlichen zu einem anderen). Zudem wäre auch in Bezug auf die Ausnahmen der Kostenlosigkeit eine andere Regelung als beim Auskunftsrecht denkbar, da hier nicht der Persönlichkeitsschutz, sondern der wirtschaftliche Wert der Daten im Vordergrund steht.
Art. 24 E-VDSG ist vollständig zu überarbeiten.

k. Art. 25 E-VDSG

Art. 25 E-VDSG hält fest, welche Aufgaben die Datenschutzberaterin oder der Datenschutzberater wahrnehmen muss. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 revDSG, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die er oder sie wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 revDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist missverständlich und zu korrigieren.

I. Art. 26 E-VDSG

In Anwendung von Art. 12 Abs. 5 revDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn (1) umfangreich besonders schützenswerte Personendaten bearbeitet werden oder (2) ein Profiling mit hohem Risiko durchgeführt wird. Wie bei Art. 4 Abs. 1 E-VDSG ist zu erwähnen, dass diese Eingrenzung bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG).

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates

Dr. iur. Roger Nobs, Ratschreiber

Kanton Bern
Canton de Berne

Regierungsrat

Postgasse 68
Postfach
3000 Bern 8
info.regierungsrat@be.ch
www.be.ch/rr

Staatskanzlei, Postfach, 3000 Bern 8

Eidgenössisches Justiz- und Polizeidepartement EJPD

jonas.amstutz@bj.admin.ch

Unser Zeichen:	2021.DIJ.4543	15. September 2021
RRB Nr.:	1075/2021	
Direktion:	Direktion für Inneres und Justiz	
Klassifizierung:	Nicht klassifiziert	

Vernehmlassung des Bundes:
Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
Stellungnahme des Kantons Bern

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Zustellung der Vernehmlassungsunterlagen zur Totalrevision der VDSG und die Einladung zur Stellungnahme. Der Regierungsrat des Kantons Bern nimmt wie folgt Stellung zur Vorlage:

1. Grundsätzliches

Der Regierungsrat begrüsst grundsätzlich die Vorlage. Allerdings geht sie aus Sicht des Regierungsrates in einigen Punkten sehr weit, da teilweise auf Verordnungsstufe neue Pflichten eingeführt werden, die wohl auf Gesetzesstufe zu regeln wären.

Der Regierungsrat bedauert zudem, dass der erläuternde Bericht mit seinen Ausführungen teilweise sehr knapp gehalten ist. Bei einigen Bestimmungen bleibt deshalb unklar, wieso diese in die Verordnung aufgenommen wurden.

Die Vorlage hat keine direkten Auswirkungen auf den Kanton Bern. Dennoch erlaubt sich der Regierungsrat als Beitrag zu einer homogenen Datenschutzgesetzgebung, wenige Anträge zu stellen. Diese konzentrieren sich auf die für Behörden anwendbare Bestimmungen, welche indirekt für die Revision des Datenschutzrechts in den Kantonen relevant sein können.

2. Anträge zu den einzelnen Bestimmungen

2.1 Zu Artikel 1 VDSG

Artikel 8 Absatz 1 nDSG verlangt von den verantwortlichen Behörden und den Auftragsbearbeitenden die Gewährleistung einer dem Risiko angemessenen Datensicherheit. Ob technische oder organisatorische Massnahmen dem Risiko angemessen sind, beurteilt sich nach den in Artikel 1 Absatz 1 VDSG festgelegten Kriterien.

2.1.1 Antrag

In Artikel 1 Absatz 1 Buchstabe d VDSG sei der Begriff «Implementierungskosten» mit «Implementierungsaufwand» zu ersetzen und Absatz 2 soll wie folgt präzisiert werden: «Die Risiken und Massnahmen sind über die gesamte Betriebsdauer hinweg in angemessenen Abständen zu überprüfen.».

2.1.2 Begründung

Der Begriff «Implementierungskosten» ist sehr eng. Um risikobasierte Massnahmen zu ergreifen, können neben den Implementierungskosten auch sonstige Implementierungskriterien relevant sein, wie beispielsweise ein hoher Personalaufwand oder zeitliche und organisatorische Aufwendungen. Der Erläuterungsbericht suggeriert auf Seite 16 ausserdem, dass die Kriterien in Absatz 1 nicht gleichwertig sind und die Implementierungskosten nicht von der Pflicht einer angemessenen Datensicherheit befreit. Diese Erläuterung ist missverständlich: Nach der Vorlage sind sämtliche in Absatz 1 aufgeführten Kriterien bei der Risikobeurteilung gleichermassen zu berücksichtigen, so auch die Implementierungskosten bzw. der Implementierungsaufwand.

Zu prüfen sind nach Absatz 2 nicht die Massnahmen, sondern vielmehr die Risikofaktoren. Die Massnahmen sind nämlich nur anzupassen, wenn sich die Risiken geändert haben. Deshalb soll Absatz 2 mit «Risiken» ergänzt werden. Damit wird verdeutlicht, was die Regelung ausdrücken will.

2.2 Zu Artikel 2 VDSG

Artikel 2 enthält eine Auflistung der Schutzziele, auf welche die organisatorischen und technischen Massnahmen auszurichten sind. Der Einleitungssatz ist unklar formuliert.

2.2.1 Antrag

Der Einleitungssatz sei wie folgt zu ändern: «Die technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit sind auf folgende Schutzziele ausgerichtet:...».

2.2.2 Begründung

Mit der Ergänzung «technisch und organisatorisch» ist klar, dass die Massnahmen gemäss Artikel 1 VDSG gemeint sind. Ausserdem können die Schutzziele – wie im Bericht erläutert – nicht in jedem Fall erreicht werden. Deshalb sollte «erreichen» mit auf folgende Schutzziele «ausgerichtet» ersetzt werden.

2.3 Zu Artikel 3 VDSG

Artikel 3 VDSG regelt die Protokollierungspflicht. Aus Sicht des Regierungsrates geht die Zweckbindung in Absatz 4 zu weit.

2.3.1 Antrag

Artikel 3 Absatz 4 sei wie folgt zu ergänzen: «Abweichende Vorgaben in der Gesetzgebung bleiben vorbehalten».

2.3.2 Begründung

Die Auswertung der Protokolldateien sollte zu weiteren Zwecken möglich sein, sofern dafür eine Rechtfertigung besteht. Bei Bundesorganen ist eine entsprechende gesetzliche Grundlage – wie beispielsweise Art. 57l des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG; SR 172.010) – erforderlich. Damit können Doppelprotokollierungen vermieden werden.

2.4 Zu Artikel 5 VDSG

Nach Artikel 5 Absatz 1 VDSG müssen Bundesbehörden weiterhin ein Bearbeitungsreglement bei automatisierten Bearbeitungen führen.

2.4.1 Antrag

Der Regierungsrat beantragt, die Bestimmungen zum Bearbeitungsreglement ersatzlos zu streichen.

Eventualiter: Der Begriff «Profiling» in Artikel 5 Bst. b VDSG sei analog Art. 4 Abs. 1 Bst. b VDSG einzuschränken.

2.4.2 Begründung

Unklar ist, wieso ein solches Bearbeitungsreglement überhaupt verlangt wird. Jedenfalls fehlt hierzu eine gesetzliche Grundlage im nDSG. Fraglich ist weiter, was der Mehrwert gegenüber dem Verzeichnis der Bearbeitungstätigkeiten nach Art. 12 nDSG wäre. Zur Erfüllung der Dokumentationspflicht genügt dieses Verzeichnis.

Zumindest ist fraglich, ob der Begriff «Profiling» hier allenfalls auch für Behörden eingeschränkt werden kann (analog zu Art. 4 Abs. 1 Bst. b VDSG). Der Begriff «Profiling» geht nach dem nDSG sehr weit, wobei anerkannt ist, dass nicht jedes Profiling mit einem hohen Risiko für die Grundrechte verbunden ist. Deshalb sollte nicht für sämtliche Profilingvarianten ein Bearbeitungsreglement erstellt werden müssen.

2.5 Zu Artikel 6 VDSG

Artikel 6 regelt die Modalitäten für die Bearbeitung durch Auftragsbearbeitende.

2.5.1 Antrag

Artikel 6 Absatz 3 sei wie folgt anzupassen: «..., so darf der Auftragsbearbeiter die Datenbearbeitung nur mit vorgängiger Genehmigung des Bundesorgans einem Dritten übertragen.».

2.5.2 Begründung

Schriftlich bedeutet sinnvollerweise «unveränderlich in Textform». Entsprechend hält der erläuternde Bericht fest, dass Schriftform insbesondere Dokumente in Papier- oder elektronischer Form meint. Um Unklarheiten vorzubeugen, sollte deshalb das Erfordernis der Schriftlichkeit gestrichen werden.

2.6 Zu Artikel 9 VDSG

Artikel 9 enthält inhaltliche Vorgaben an die Datenschutzklauseln in Verträgen, die zu einer Bekanntgabe in einen Staat ohne angemessenes Schutzniveau legitimieren.

2.6.1 Antrag

Artikel 9 Absatz 1 Buchstabe j VDSG sei ersatzlos zu streichen.

2.6.2 Begründung

Die Informationspflichten obliegen gemäss Artikel 19 bis Artikel 23 nDSG nur den verantwortlichen Behörden. Eine Ausdehnung der Pflicht auf die Datenempfängerin bzw. den Datenempfänger scheint wenig sinnvoll und ist wohl auch nicht praktikabel.

2.7 Zu Artikel 13 VDSG

Artikel 13 VDSG regelt die Modalitäten der Informationspflicht.

2.7.1 Antrag

In Absatz 1 zu Artikel 13 sei «der Auftragsbearbeiter» zu streichen.

2.7.2 Begründung

Die Informationspflicht obliegt gemäss Artikel 19 ff. nDSG nur den verantwortlichen Behörden, jedoch nicht den Auftragsbearbeitenden. Diese müssen sich lediglich an die vertraglichen Pflichten bzw. an die gesetzlichen Vorgaben (bei Übertragung der Aufgabe im Gesetz) halten.

2.8 Zu Artikel 15 VDSG

Artikel 15 regelt die Bekanntgabe bzw. Weitergabe von Personendaten.

2.8.1 Antrag

Die Bestimmung sei ersatzlos zu streichen.

Eventualiter: «Auftragsbearbeiter» sei zu streichen.

2.8.2 Begründung

Gemäss Artikel 6 Absatz 5 nDSG muss sich, wer Personendaten bearbeitet, über deren Richtigkeit vergewissern. Das gilt auch für die Bekanntgabe von Personendaten. Die zusätzliche Informationspflicht an die Empfängerin bzw. den Empfänger ist deshalb überflüssig und die Bestimmung könnte gestrichen werden. Mindestens zu streichen ist jedenfalls der Begriff «Auftragsbearbeiter», da die Informationspflichten nach nDSG für ihn bzw. sie nicht gelten (vgl. Ziff. 2.7).

2.9 Zu Art. 16 VDSG

Artikel 16 regelt die Informationspflicht im Fall der Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten.

2.9.1 Antrag

Artikel 16 sei ersatzlos zu streichen.

2.9.2 Begründung

Der Vernehmlassungsentwurf zum nDSG sah entsprechende Informationspflichten vor. Diese fanden jedoch keinen Eingang in das nDSG. Es fehlt daher eine gesetzliche Grundlage zum Erlass dieser Bestimmung, weshalb diese ersatzlos gestrichen werden sollte.

2.10 Zu Art. 18 VDSG

Artikel 18 regelt die Form und Aufbewahrung der Datenschutz-Folgeabschätzung.

2.10.1 Antrag

Der erste Satz von Artikel 18 VDSG sei wie folgt zu ändern: Der bzw. die Verantwortliche «muss die Datenschutz-Folgeabschätzung in nachvollziehbarer Weise festhalten.».

2.10.2 Begründung

Das Erfordernis der Schriftlichkeit sollte mit «in nachvollziehbarer Weise» ersetzt werden, um Unklarheiten vorzubeugen. Damit ist klar, dass die Dokumentation sowohl in Papier- als auch elektronischer Form erfolgen kann (vgl. auch Ziff. 2.5).

2.11 Zu Artikel 20 VDSG

Artikel 20 VDSG regelt die Modalitäten des Auskunftsrechts.

2.11.1 Antrag

Absatz 3 von Artikel 20 VDSG sei wie folgt anzupassen: «Die Auskunft muss allgemein verständlich sein.».

2.11.2 Begründung

Würde – wie im Entwurf vorgeschlagen – die Auskunft für die betroffene Person verständlich sein müssen, so wären die Verantwortlichen verpflichtet, sich an den Fähigkeiten der betroffenen Person zu orientieren. Die Bestimmung ist dahingehend zu präzisieren, dass die Auskunft für eine durchschnittlich betroffene Person verständlich sein muss.

3. Weiteres

Sowohl der Verordnungsentwurf als auch der erläuternde Bericht lassen teilweise eine geschlechtsneutrale Sprache vermissen.

3.1 Antrag

Der Verordnungsentwurf und der erläuternde Bericht seien auf eine geschlechtsneutrale Sprache zu prüfen.

3.2 Begründung

In Artikel 15 VDSG findet sich beispielsweise folgende Formulierung: «Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger». Gendergerechter wäre die Formulierung «die verantwortliche Person» oder «die auftragsgebende Person». Dem Regierungsrat ist bewusst, dass es sich hier um im nDSG definierte Begriffe handelt. Dennoch erachtet er eine gendergerechte Formulierung als prüfenswert.

3.3 Antrag

Der Regierungsrat unterstützt die weiteren Anträge und Hinweise gemäss Stellungnahme der Konferenz der schweizerischen Datenschutzbeauftragten (privatim) vom 1. September 2021 (Beilage), mit Ausnahme der Streichung von Art. 20 Abs. 3 VDSG.

3.4 Begründung

Die von einem anerkannten Datenschützer im Auftrag von privatim erarbeitete Stellungnahme zeigt eine Reihe von rechtstechnischen Mängel des Vorentwurfs auf. Die Anträge des Kantons Bern und von privatim sind weitestgehend komplementär. Lediglich bei Art. 20 Abs. 3 VDSG führen die gleichen Einwände zu unterschiedlichen Anträgen, wobei der Antrag des Kantons Bern in Ziff. 2.11 vorzuziehen ist.

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates

Beatrice Simon
Regierungspräsidentin

Christoph Auer
Staatsschreiber

Beilage
- Stellungnahme der Konferenz der schweizerischen Datenschutzbeauftragten (privatim) vom 1. September 2021

Verteiler
- Finanzdirektion
- Gesundheits-, Sozial- und Integrationsdirektion
- Sicherheitsdirektion
- Datenschutzaufsichtsstelle

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail:
jonas.amstutz@bj.admin.ch

Bern, 1. September 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassungsverfahren

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) Stellung nehmen zu können. Gerne äussern wir uns dazu wie folgt:

1. Allgemeines

Das revidierte Bundesgesetz über den Datenschutz vom 25.09.2020 (revDSG) beinhaltet zahlreiche Delegationsnormen, auf die sich der vorliegende E-VDSG stützt (siehe Ingress E-VDSG). Zudem konkretisiert der E-VDSG verschiedene Bestimmungen des revDSG.

Insgesamt entsteht der Eindruck einer Verordnung, die (zu) wenig Klarheit für die Umsetzung durch die Verantwortlichen schafft. Einerseits liegt es darin, dass überholte Begriffe und Bestimmungen der bisherigen Verordnung einfach übernommen werden. Andererseits bringen die neuen Bestimmungen nicht die notwendige Detaillierung für die Umsetzung des an sich schon komplexen revDSG.

Die Verantwortlichen – private Personen wie auch Bundesorgane – werden Mühe haben, verschiedene dieser Bestimmungen angemessen umzusetzen.

Das Konzept der E-VDSG und einzelne Bestimmungen sollten deshalb im Hinblick auf eine wirkungsvolle Umsetzung des Datenschutzes grundsätzlich überprüft werden.

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, CH-3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

2. Einzelne Bestimmungen

a. Art. 1 bis 4 E-VDSG (Datensicherheit)

Die Art. 1 bis 4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 revDSG). Dabei verlangt Art. 8 Abs. 3 revDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt.

Der E-VDSG verpasst es, diese Mindestanforderungen in einer Form zu konkretisieren, die auch in Bezug auf die strafbewehrte Unterlassung der Umsetzung der Mindestanforderungen (Art. 61 Abs. 1 Bst. c revDSG) objektive Tatbestandsmerkmale erkennen lassen würde. In Bezug auf die Datensicherheit ist in der Informationsbearbeitung heute ein Standard erreicht, der klar nach der Beurteilung des Schutzbedarfs und der Risiken die entsprechenden Sicherheitsmassnahmen vorschlägt und einteilt (Grundschutz, hoher Schutz, sehr hoher Schutz). Der Bund hat soeben mit der Verabschiedung des Bundesgesetzes über die Informationssicherheit (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020) gezeigt, wie die heutigen Anforderungen auch gesetzestechnisch umgesetzt werden können.

Der E-VDSG hält dagegen am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht, ohne aber Art. 8 revDSG für die Praxis zu konkretisieren.

Der Abschnitt 1 (Datensicherheit) ist aus unserer Sicht konzeptionell grundsätzlich zu überarbeiten.

b. Art. 1 E-VDSG

Art. 1 Abs. 1 E-VDSG schreibt eine Beurteilung der Angemessenheit von Massnahmen nach den Kriterien Zweck, Art, Umfang und Umstände der Datenbearbeitung, Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen, Stand der Technik und Implementierungskosten vor.

Hier wird im Wesentlichen Art. 32 DSGVO rezipiert, ohne aber das in diesem Artikel formulierte Ziel in den Vordergrund zu stellen: «ein dem Risiko angemessenes Schutzniveau zu gewährleisten».

Mitunter bedeutet dies, dass die Schutzziele, der Schutzbedarf und die Risiken zuerst zu beurteilen sind.

Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt, wie dies auch die Erläuterungen erwähnen (S. 15) und werden in Art. 2 E-VDSG ausführlich aufgezählt (siehe nachfolgend Art. 2 E-VDSG). Der Schutzbedarf ergibt sich aus der Art der Daten (Personendaten, besonders schützenswerte Personendaten) und der Datenbearbeitung selbst (z.B. Profiling). Erst dann erfolgt die Risikobeurteilung, wie dies auch die Datenschutz-Folgenabschätzung vorsieht (Art. 22 revDSG).

Die Kriterien «Zweck, Art, Umfang und Umstände der Datenbearbeitung» beziehen sich somit auf die Schutzbedarfsfeststellung (welche bereits eine erste grobe Einschätzung des möglichen Schadensausmasses enthält), die Kriterien «Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen» auf die Risikobeurteilung.

Wenn es um die Beurteilung der Angemessenheit der Massnahmen geht, sind die Kriterien «Stand der Technik und Implementierungskosten» einschlägig. Sie sagen aber nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche dem Risiko mit der nötigen Effektivität begegnet. Dies ist im erwähnten ISG so angelegt, aber auch in Art. 32 DSGVO, der hier zitiert wird (Erläuterungen, S. 15).

Art. 1 Abs. 1 E-VDSG ist deshalb konzeptionell grundsätzlich zu überarbeiten.

Art. 1 Abs. 2 E-VDSG verlangt, dass die Massnahmen über die gesamte Bearbeitungszeit in angemessenen Abständen zu überprüfen sind. Diese Formulierung greift zu kurz. In erster Linie ist die Risikobeurteilung laufend zu überprüfen, woraus sich die Massnahmen und deren Angemessenheit ergeben und somit die allfällige Anpassung von Massnahmen.

Die Formulierung ist zu korrigieren.

c. Art. 2 E-VDSG

Die Aufzählung der Schutzziele wurde aus der geltenden Verordnung übernommen und mit Bestimmungen aus der DSGVO ergänzt.

Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt und lassen sich in die in der Informatiksicherheit üblichen Schutzziele zusammenfassen: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit (so auch Erläuterungen, S. 15). Er erscheint als angezeigt, dies entsprechend klar zum Ausdruck zu bringen (vgl. in diesem Sinne Art. 6 Abs. 2 des Informationssicherheitsgesetzes vom 18.12.2020).

Die in Art. 2 aufgeführten Vorgaben stellen keine eigenständigen Schutzziele dar, sondern Anforderungen an die Massnahmen, welche zur Erreichung der Schutzziele zu treffen sind (so stellt etwa die Zugriffskontrolle kein Schutzziel dar, sondern eine Anforderung zur Gewährleistung der Vertraulichkeit im Rahmen des Verhältnismässigkeitsprinzips).

Zudem ist der Einleitungssatz von Art. 2 E-VDSG missverständlich. Schutzziele sind Zielvorgaben. Die Massnahmen müssen angemessen sein in Bezug auf die in der Risikobeurteilung festgestellten Risiken und nicht in Bezug auf die Schutzziele.

d. Art. 3 E-VDSG

Art. 3 E-VDSG sieht insbesondere für Bundesorgane eine ausführliche Protokollierung der Datenbearbeitungen vor.

Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und dann unter Umständen sanktioniert) werden kann. Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das mittels Protokollierung wirksam reduziert werden kann; dass ein *irgendwie* geartetes Risiko verbleibt, reicht nicht (es fehlt dann an der Verhältnismässigkeit der neuen Datenbearbeitung). Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen zu umfassende Berechtigungen implementiert werden müssen, weil nicht zum Vorherein bekannt ist, auf welche konkreten Daten

der/die Berechtigte bei der Aufgabenerfüllung Zugang haben muss (z.B. im Schengen-Informationssystem). Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert und stichprobenweise überprüft werden. Die Pflicht zur Protokollierung als kompensierende Massnahme ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert.

Für die Bundesorgane soll die Protokollierung für das Bearbeiten sämtlicher Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Hier wird weit über das Ziel hinausgeschossen. Die Protokollierung stellt selbst eine Beschaffung von Personendaten dar, die dem Grundsatz der Verhältnismässigkeit genügen muss. Zwar erlaubt Art. 57*l* Bst. b Ziff. 4 RVOG die Aufzeichnung von Randdaten zum Nachvollzug des Zugriffs auf Datensammlungen, aber eben nur insoweit, als die Aufzeichnung verhältnismässig ist. Dass selbst bei einfachen Personendaten und selbst bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht klar über diese Anforderung hinaus. Die Bundesorgane sind deshalb in Absatz 1 aufzunehmen und auf Absatz 2 ist zu verzichten.

In Art. 3 Abs. 3 E-VDSG sollte vor «die Identität der Empfängerin oder des Empfängers» das Wort «gegebenenfalls» eingefügt werden, da es sich nicht bei jeder protokollierten Bearbeitung um eine Bekanntgabe handelt.

Gemäss Art. 3 Abs. 4 E-VDSG sind die Protokolle während zweier Jahre aufzubewahren und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei ist nicht in jedem Fall eine personenbezogene Auswertung erforderlich. Für die Bundesorgane legen die Art. 57*m* ff. RVOG und Art. 8 ff. der zugehörigen Ausführungsverordnung fest, wie die Auswertungen erfolgen dürfen, wobei ggf. auch ein gestaffeltes Vorgehen angezeigt ist (vgl. BGE 143 II 443). Der letzte Satz ist deshalb im Sinne «dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden» zu ergänzen.

e. Art. 4 E-VDSG

Die Erstellung eines Bearbeitungsreglements wird für private Verantwortliche und deren Auftragsbearbeiter vorgesehen, die (1) umfangreich besonders schützenswerte Personendaten bearbeiten oder (2) ein Profiling mit hohem Risiko durchführen (Art. 4 Abs. 1 E-VDSG). Diese Eingrenzung erscheint willkürlich und deckt bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen ab.

Hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG). Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 revDSG), die Teil des Bearbeitungsreglements sein können.

Art. 4 Abs. 2 E-VDSG enthält Mindestangaben für das Datenbearbeitungsreglement. Auch hier wird kein Konnex zu den Standards in der Informatik gemacht, in dem auf diese verwiesen würde. Dann würde es genügen, auf die spezifischen datenschutzrechtlichen Vorgaben hinzuweisen (Bst. h, j).

Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater ist die Fachperson bei einem Verantwortlichen und ein Bearbeitungsreglement wird zusammen mit ihr/ihm erstellt und nicht «der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung» gestellt. Es gehört zu den Aufgaben der Datenschutzberaterin oder des Datenschutzberaters, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b revDSG). Zudem hat die Datenschutzberaterin oder der Datenschutzberater über die erforderlichen Fachkenntnisse zu verfügen (Art. 10 Abs. 3 Bst. c revDSG), weshalb die Formulierung, das Bearbeitungsreglement sei ihr oder ihm «in verständlicher Form» zur Verfügung zu stellen, offensichtlich eine Abwertung seiner Fachkompetenzen impliziert.

Art. 4 Abs. 3 E-VDSG ist ersatzlos zu streichen.

f. Art. 5 E-VDSG

Grundsätzlich kann auf unsere Ausführungen zu Art. 4 E-VDSG verwiesen werden.

g. Art. 7 E-VDSG

Auch die Datenschutzberaterin oder der Datenschutzberater des Bundesorgans hat bei der Anwendung der Datenschutzvorschriften mitzuwirken (vgl. unten Art. 28 E-VDSG). Es widerspricht dem präventiven und risikoorientierten Ansatz des revDSG, wenn die Datenschutzberaterin oder der Datenschutzberater lediglich nachträglich über den Abschluss eines Outsourcingvertrags oder bei einer Funktionsübertragung informiert werden soll. Zu den Aufgaben einer Datenschutzberaterin oder eines Datenschutzberaters gehört die Involvierung in solche Geschäfte. Die ist eine Kernaufgabe der Beraterin oder des Beraters («Mitwirkung bei der Anwendung der Datenschutzvorschriften»). Die Datenschutzberaterin oder der Datenschutzberater ist rechtzeitig zu informieren, wie dies korrekterweise bei Datenbearbeitungsprojekten vorgesehen ist (Art. 31 E-VDSG).

Art. 7 E-VDSG ist ersatzlos zu streichen.

h. Art. 8 E-VDSG

Bei den Formulierungen in Art. 8 E-VDSG fällt auf, dass der EDÖB konsultiert wird (formell), und die Beurteilungen von internationalen Organisationen oder ausländischen Behörden berücksichtigt werden können (materiell). Es ist klar zu formulieren, dass auch die Stellungnahmen des EDÖB materiell zu berücksichtigen sind, zumal sich die Erläuterungen hierzu nicht äussern (Erläuterungen, S. 27).

i. Art. 9 Abs. 3 E-VDSG

Gemäss Art. 16 Abs. 2 Bst. b und c revDSG sind Datenschutzklauseln und spezifische Garantien dem EDÖB vorgängig mitzuteilen. Der Einleitungssatz von Art. 9 Abs. 3 E-VDSG suggeriert, dass es einen Sachverhalt geben könnte, in der auch die Nicht-Mitteilung zu einer rechtskonformen Bekanntgabe ins Ausland führen würde.

Die Formulierung ist anzupassen.

j. Art. 19 E-VDSG

Art. 24 Abs. 1 revDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 revDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 revDSG).

Art. 24 revDSG ist eine (bewusst) abweichende Bestimmung von Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO rezipiert. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen. Für die Mehrheit der Verantwortlichen ist dies aber nicht der Fall und Art. 19 E-VDSG bringt unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde rasch informiert wird, allenfalls auch die betroffenen Personen, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden.

Art. 24 revDSG braucht die in Art. 19 E-VDSG enthaltene Konkretisierung nicht.

k. Art. 20 E-VDSG

Art. 25 revDSG und Art. 26 revDSG regeln das Auskunftsrecht und dessen Einschränkungen ausführlich. Art. 20 E-VDSG bringt hierzu einige Konkretisierungen, die aber über das Notwendige hinausgehen.

Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 revDSG definiert. Daraus ergeben sich der Umfang und der Zweck der Auskunft. Dies misst sich nach objektiven Kriterien. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte.

Art. 20 Abs. 3 E-VDSG ist ersatzlos zu streichen.

Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen». Dies ergibt sich bereits aus Art. 8 revDSG und den Bestimmungen des 1. Kapitels der E-VDSG.

Diese Erwähnung ist in Art. 20 Abs. 4 E-VDSG zu streichen.

Art. 26 Abs. 4 revDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person.

Art. 20 Abs. 5 E-VDSG ist ersatzlos zu streichen.

l. Art. 21 E-VDSG

Art. 21 Abs. 1 E-VDSG sieht vor, dass ein Verantwortlicher, der für die Behandlung des Begehrens nicht zuständig, dieses an den zuständigen Verantwortlichen weiterleitet. Dieser verwaltungsrechtliche Grundsatz gilt für die Bundesorgane auch ohne Erwähnung in diesem Zusammenhang. Im öffentlich-rechtlichen Bereich ergibt er sich aus dem hoheitlichen Verhältnis der Bürgerinnen und Bürger zum Staat. Im privatrechtlichen Verhältnis legen die Parteien ihre Rechte und Pflichten aber autonom fest. Die gleiche Auflage auch dem privatrechtlichen Verantwortlichen zu machen, ist unverhältnismässig. Sie führt zu einem Aufwand für den privatrechtlichen Verantwortlichen, den «zuständigen» Verantwortlichen ausfindig zu machen, ohne dass dadurch die Rechte der betroffenen Personen gestärkt würden.

Art. 21 Abs. 1, 2. Satz E-VDSG ist ersatzlos zu streichen.

m. Art. 24 E-VDSG

Art. 24 E-VDSG beinhaltet eine Konkretisierung von Art. 28 revDSG, indem er sich auf die sinngemässe Anwendung von Bestimmungen zum Auskunftsrecht verweist. Dies wird dem neuen Rechtsinstitut der «Datenportabilität» nicht gerecht und verkennt den durchaus vorhandenen Bedarf einer Konkretisierung der gesetzlichen Bestimmung (beispielsweise in Bezug auf die «gängigen elektronischen Formate» oder den «unverhältnismässigen Aufwand» bei der direkten Übertragung von einem Verantwortlichen zu einem anderen). Zudem wäre auch in Bezug auf die Ausnahmen der Kostenlosigkeit eine andere Regelung als beim Auskunftsrecht denkbar, da hier nicht der Persönlichkeitsschutz, sondern der wirtschaftliche Wert der Daten im Vordergrund steht.

Art. 24 E-VDSG ist vollständig zu überarbeiten.

n. Art. 25 E-VDSG

Art. 25 E-VDSG hält fest, welche Aufgaben die Datenschutzberaterin oder der Datenschutzberater wahrnehmen muss. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 revDSG, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die er oder sie wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 revDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist missverständlich und zu korrigieren.

o. Art. 26 E-VDSG

In Anwendung von Art. 12 Abs. 5 revDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn (1) umfangreich besonders schützenswerte Personendaten bearbeitet werden oder (2) ein Profiling mit hohem Risiko durchgeführt wird. Wie bei Art. 4 Abs. 1 E-VDSG ist zu erwähnen, dass diese Eingrenzung bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es angezeigt, die Voraussetzungen

für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG).

p. Art. 28 E-VDSG

Art. 28 E-VDSG legt die Aufgaben der Datenschutzberaterin oder -beraters der Bundesorgane fest. In der Aufzählung von Art. 28 Abs. 2 E-VDSG fällt auf, dass die in Art. 10 Abs. 2 Bst. b revDSG festgelegte Aufgabe – die Mitwirkung bei der Anwendung der Datenschutzvorschriften – nicht erwähnt wird, sondern nur die Schulung und Beratung (Art. 10 Abs. 2 Bst. a revDSG). Wir gehen davon aus, dass es sich hier um ein Versehen handelt, ist doch die Mitwirkung bei der Anwendung der Datenschutzvorschriften eine Kernaufgabe von Datenschutzberaterinnen und -berater. Diese Aufgabe ist in Art. 28 Abs. 2 E-VDSG zu ergänzen.

q. Art. 36 E-VDSG

Die Bestimmung ist überflüssig, weil sich diese Präzisierung bereits aus Art. 39 revDSG klar ergibt.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim

Landeskanzlei
Rathausstrasse 2
4410 Liestal
061 552 50 06
landeskanzlei@bl.ch
www.bl.ch

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat BL, Rathausstrasse 2, 4410 Liestal

Eidgenössisches
Justiz- und Polizeidepartement
Bern
jonas.amstutz@bj.admin.ch

Liestal, 28. September 2021

Vernehmlassung
zum Entwurf einer Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin

Besten Dank für die Möglichkeit zur Stellungnahme, zum erwähnten Verordnungsentwurf teilen wir Folgendes mit:

A. Grundsätzliche Bemerkungen

Die Präzisierung des Bundes-Datenschutzrechts ist zu begrüssen, auch wenn dieses die Kantone nur mittelbar tangiert. Bekanntlich ist ja für die Datenbearbeitungen durch kantonale und kommunale öffentliche Organe das Datenschutzrecht des Kantons massgebend. Dennoch wird bei der Auslegung kantonaler Regelungen auch die Auslegung entsprechender Bundesnormen hinzugezogen, sodass gewisse Bestimmungen des Bundesrechts auch für die Kantone besondere Relevanz erhalten.

B. Bemerkungen zu einzelnen Bestimmungen des Verordnungsentwurfs

Vorbemerkung: Über die basellandschaftliche Aufsichtsstelle Datenschutz erhielten wir Kenntnis von der Stellungnahme, welche die Konferenz der Schweizerischen Datenschutzbeauftragten «privatim» im Rahmen des laufenden Vernehmlassungsverfahren beim Eidgenössischen Justiz- und Polizeidepartement eingereicht hat. Nach Konsultation unserer Aufsichtsstelle können wir uns den darin enthaltenen Feststellungen anschliessen. Dies betrifft insbesondere die Beobachtung, dass die Verordnung des Bundes die im revidierten Datenschutzgesetz verfolgte Grundrichtung eines risikobasierten Ansatzes nicht klar genug wiedergibt, indem sie etwa Massnahmen wie die Protokollierung (Artikel 3 Revisionsentwurf) generell vorschreibt, ohne deren Zweckmässigkeit für die Senkung eines Risikos zu beurteilen. Weiter möchten wir folgende Aspekte
zu ersten drei Bestimmungen des Revisionsentwurfs herausheben, die für die kantonale Praxis besonders relevant sind:

Artikel 1 und 2 des Revisionsentwurfs: Die Festlegung der Grundsätze sowie die Festlegung der Schutzziele werden einen Einfluss auf die Projektmethodik haben, die auf Bundesebene verwendet wird. Der Kanton Basel-Landschaft schreibt derzeit für die meisten Projekte die gleiche Projektmethode wie der Bund vor (HERMES). Deshalb ist es für unseren Kanton entscheidend, dass Artikel 1 die Risikobeurteilung und die zu ergreifenden Massahmen auf dem aktuellen Stand der fachlichen Diskussion wiedergibt. So werden in Artikel 2 – entgegen den Ausführungen des Erläuternden Berichts zu Artikel 1 – die etablierten Schutzziele «Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit» nicht ausdrücklich erwähnt. Wir schlagen vor, die Artikel 1 und 2 des Revisionsentwurfs zu überarbeiten. Besonderes Augenmerk sollte auf den Standardprozess zur Festsetzung der angemessenen Schutzmassnahmen gelegt werden. Ausgehend vom Schutzbedarf der Daten werden die Risiken ermittelt und darauf basierend die organisatorischen und technischen Massnahmen zur Reduktion dieser Risiken definiert.

Artikel 3 des Revisionsentwurfs: Eine generelle Pflicht zur Protokollierung von Zugriffen unabhängig von der Zweckmässigkeit für die Reduktion eines Risikos führt zu einer umfangreichen neuen Datensammlung (z.B. mit Daten von Anwendenden/Mitarbeitenden im Kanton bei der Verwendung von Bundessystemen) mit einer sehr langen Aufbewahrungsdauer. Diese Normierung erweist sich somit als unverhältnismässig. Die Protokollierung muss immer risikobasiert erfolgen und ist erst zweite Wahl, sofern unberechtigte Zugriffe technisch nicht ausreichend eingeschränkt werden können

Abschliessend bedanken wir uns nochmals für die Gelegenheit zur Meinungsäusserung und für eine wohlwollende Prüfung unserer Anliegen.

Hochachtungsvolls

Thomas Weber
Regierungspräsident

Elisabeth Heer Dietrich
Landschreiberin

Regierungsrat des Kantons Basel-Stadt

Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

Eidgenössisches Justiz- und Polizeidepartement
Frau Bundesrätin Karin Keller-Sutter

per E-Mail an jonas.amstutz@bj.admin.ch

Basel, 19. Oktober 2021

Regierungsratsbeschluss vom 19. Oktober 2021
Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG): Stellungnahme des Kantons Basel-Stadt

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Juni 2021 haben Sie uns die Vernehmlassungsunterlagen zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) zukommen lassen. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und lassen Ihnen nachstehend unsere Anträge und Bemerkungen zukommen.

1. Grundsätzliche Einschätzung

Der Regierungsrat begrüsst grundsätzlich die Novellierung der VDSG, welche aufgrund der 2020 von den Eidgenössischen Räten beschlossenen Revision des Bundesgesetzes über den Datenschutz (DSG) notwendig geworden ist. Der Entwurf erscheint indessen generell als sehr umfangreich. Es ist fraglich, ob ein so hoher Detaillierungsgrad in einer Verordnung wünschenswert ist.

Wie das Datenschutzgesetz des Bundes hat auch die entsprechende Ausführungsverordnung kaum unmittelbare Auswirkungen auf die Kantone, da diese wie auch die Gemeinden von deren Geltungsbereich nicht erfasst sind. Allerdings ergibt sich die Anwendbarkeit des DSG und damit auch der VDSG aufgrund des kantonalen Rechts in gewissen Fällen: § 2 Abs. 2 lit. a des baselstädtischen Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (SG 153.260) schliesst dessen Anwendung aus, soweit ein kantonales öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt. In diesen Fällen, in welchen die öffentlichen Organe wie Private handeln, ist das Datenschutzrecht des Bundes anwendbar. Wir fokussieren daher im Folgenden auf Bestimmungen im Entwurf zur Totalrevision der VDSG (E-VDSG), welche in diesem Zusammenhang von Bedeutung sein können.

2. Anträge zu den einzelnen Änderungsvorschlägen

2.1 Artikel 19 E-VDSG

Antrag:
Wir beantragen, Abs. 1 ersatzlos zu streichen.

Begründung:
Art. 24 Abs. 2 der Neufassung des Bundesgesetzes über den Datenschutz vom 25. September 2020 (nDSG) nennt die Mindestanforderungen an eine Meldung von Verletzungen der Datensicherheit. Diese Bestimmung erscheint klar und in praktisch jedem Einzelfall auch umsetzbar. Art. 19 Abs. 1 E-VDSG stellt keine blosse Konkretisierung dieser Bestimmung dar, sondern geht mit einem umfangreichen Anforderungskatalog weit über die gesetzliche Regelung hinaus. Mehrere der Anforderungen werden durch den Einschub «soweit möglich» ergänzt, wodurch deutlich wird, dass die Umsetzung dieser Anforderungen im Einzelfall schwierig oder unmöglich sein kann. Zu hohe Anforderungen an den Inhalt der Meldung können aber kontraproduktiv sein, da es für die Wirksamkeit der Meldepflicht wesentlich ist, dass die Meldungen rasch und verlässlich erfolgen. Da die Anforderungen an den Inhalt der Meldungen in Art. 24 Abs. 2 nDSG keiner Konkretisierung bedürfen, ist auf Art. 19 Abs. 1 E-VDSG zu verzichten.

2.2 Artikel 20 E-VDSG

Antrag:
Wir beantragen, Abs. 3 ersatzlos zu streichen.

Begründung:
Art. 25 f. nDSG regeln das Auskunftsrecht der betroffenen Person und dessen Einschränkungen ausführlich. Eine weitere Konkretisierung auf Verordnungsebene erscheint generell wenig notwendig. Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Verständlichkeit ist ein subjektives Kriterium. Art. 25 Abs. 2 nDSG definiert indessen objektiv, worin die Information der betroffenen Person bestehen muss. Zweck der Bestimmung ist, dass diese ihre gesetzlichen Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Das Erfordernis der Verständlichkeit würde bedeuten, dass der Verantwortliche die Information vor der Auskunftserteilung unter Umständen bearbeiten muss. Dies würde nicht nur einen unangemessenen Zusatzaufwand bedeuten, es widerspricht auch dem Zweck, dass die betroffene Person durch die Auskunftserteilung Einsicht in die Informationen erhält, so, wie sie beim jeweiligen Bundesorgan oder Privaten vorhanden sind.

Antrag:
Wir beantragen, Abs. 5 folgendermassen zu ändern:

«Der Verantwortliche ~~hat~~ muss über die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft ~~zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren~~ schriftlich Auskunft erteilen.

Begründung:
Der erläuternde Bericht hält auf Seite 36 zutreffend fest, dass aus Beweisgründen eine schriftliche Auskunftserteilung über die Gründe einer Verweigerung, Einschränkung oder eines Aufschubs der Auskunft angezeigt ist, erwähnt aber auch die Möglichkeit einer mündlichen Auskunftserteilung. Nur eine schriftliche Auskunft ermöglicht es aber der betroffenen Person gegebenenfalls, ihre Rechte durchzusetzen. Eine bloss mündliche Auskunftserteilung ist daher auszuschliessen. Wird die Auskunft aber stets schriftlich erteilt, so besteht kein Bedarf für eine besondere Regelung einer Dokumentationspflicht.

2.3 Artikel 21 E-VDSG

Antrag:
Wir beantragen, den zweiten Satz von Abs. 1 ersatzlos zu streichen.

Begründung:
Art. 21 Abs. 1 E-VDSG sieht vor, dass ein Verantwortlicher, der für die Behandlung des Begehrens nicht zuständig ist, dieses an den zuständigen Verantwortlichen weiterleitet. Dieser verwaltungsrechtliche Grundsatz gilt für die Bundesorgane auch ohne Erwähnung in diesem Zusammenhang. Im privatrechtlichen Verhältnis legen die Parteien ihre Rechte und Pflichten aber autonom fest. Die gleiche Auflage auch privatrechtlichen Verantwortlichen zu machen, ist unverhältnismässig. Sie führt unter Umständen zu einem beträchtlichen Aufwand für privatrechtliche Verantwortliche, den «zuständigen» Verantwortlichen oder die «zuständige» Verantwortliche ausfindig zu machen, ohne dass dadurch die Rechte der betroffenen Personen wesentlich gestärkt würden.

2.4 Artikel 25 E-VDSG

Antrag:
Wir beantragen, Abs. 1 ersatzlos zu streichen.

Begründung:
Art. 10 Abs. 2 nDSG regelt bereits die Aufgaben der Datenschutzberaterin oder des Datenschutzberaters. Die generellere, umfassendere Formulierung dieser Bestimmung ist Art. 25 Abs. 1 E-VDSG vorzuziehen und bedarf keiner Konkretisierung. Zudem ist dem Gesetz kein Auftrag zur Regelung einer allgemeinen Überprüfung sämtlicher Bearbeitungen von Personendaten, wie sie Art. 25 Abs. 1 lit. a E-VDSG verlangt, zu entnehmen. Eine solch umfassende Prüfungspflicht erscheint als unverhältnismässig.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Für Rückfragen steht Ihnen gerne der Rechtsdienst der Staatskanzlei, Herr Patrick von Hahn, patrick.vonhahn@bs.ch, Tel. 061 267 80 59, zur Verfügung.

Freundliche Grüsse
Im Namen des Regierungsrates des Kantons Basel-Stadt

Beat Jans
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin

ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat CE
Staatsrat SR

Rue des Chanoines 17, 1701 Fribourg

T +41 26 305 10 40, F +41 26 305 10 48
www.fr.ch/ce

Conseil d'Etat
Rue des Chanoines 17, 1701 Fribourg

PAR COURRIEL

Département fédéral de justice et police
Madame la Conseillère fédérale
Karin Keller-Sutter
Palais fédéral ouest
3003 Berne

Courriel : jonas.amstutz@bj.admin.ch

Fribourg, le 12 octobre 2021

Projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Madame la Conseillère fédérale,

La procédure de consultation liée à l'avant-projet d'Ordonnance fédérale relative à la Loi fédérale sur la protection des données (P-OLPD) a retenu toute notre attention. Après consultation des instances cantonales concernées, le Conseil d'Etat fribourgeois a l'avantage de vous faire part de ses observations sur le projet présenté.

Remarques d'ordre général

Compte tenu des changements de paradigmes dans ce domaine et de l'impact pour les responsables de traitements, nous saluons toute avancée rapide dans la détermination des exigences légales fédérales en matière de protection des données. Nous observons favorablement que dans votre projet d'ordonnance certaines nouvelles dispositions restent assez ouvertes, de manière à laisser une marge de manœuvre dans la mise en œuvre des mesures techniques ou organisationnelles.

Occupés à la révision de notre propre législation cantonale en matière de protection des données, nous comptons trouver dans la version définitive de la future OLPD des lignes directrices empreintes de pragmatisme sur lesquelles nous pourrons également nous appuyer. La transversalité de nombreux projets comme les exigences internationales dans les traitements de données personnelles nous poussent à adopter une vision cohérente pour couvrir les risques d'atteinte aux droits fondamentaux.

Au vu du champ d'application, vous trouvez quelques remarques ciblées de notre Service de législation liées au contenu ou à l'interprétation de certaines dispositions qui pourraient par ailleurs impacter notre propre législation cantonale.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.

Au nom du Conseil d'Etat :

Jean-François Steiert, Président

Danielle Gagnaux-Morel, Chancelière d'Etat

L'original de ce document est établi en version électronique

Annexe

—

Remarques spécifiques de notre Service de législation

Remarques spécifiques de notre Service de législation

Suppression des dispositions concernant les identifiants de personnes (art. 25 de l'actuelle OLPD)

La suppression de cette disposition peut sembler motivée, d'une part, par la non-reprise dans la nouvelle LPD de l'article 36 al. 4 let. c de l'actuelle LPD et, d'autre part, par l'illusion que le NAVS dans sa nouvelle réglementation pourrait remplacer tous les identifiants existants. Ce deuxième élément semble néanmoins plus qu'incertain. D'une part, le PFPDT pousse toujours à la création d'identifiants sectoriels et, d'autre part, beaucoup d'entités (aussi cantonales, même si elles peuvent dans ce domaine se référer à leurs propres règles) continueront en pratique à travailler en parallèle avec des identifiants sectoriels.

La création et l'utilisation d'identifiants partagés par plusieurs entités différentes devraient continuer à être réglementées tant du point de vue de la légalité que de celui du respect des droits fondamentaux. Afin de ne pas laisser se développer un vide juridique autour de ce traitement spécifique de données, il conviendrait de réintroduire des règles à ce sujet dans la future OLPD.

Article 19 P-OLPD

Il faudrait éviter que toute annonce se retrouve sur la place publique de manière prématurée. Dans un arrêt récent, le Tribunal fédéral a jugé qu'une annonce des violations de la sécurité des données correspond à un document officiel soumis au principe de la transparence (ATF 1C_500/2020 du 11 mars 2021). Alors que cette annonce est faite aujourd'hui sur une base totalement volontaire par le responsable de traitement, son contenu peut donc par principe être transmis à quiconque en fait la demande (en plus du PFPDT) sur la base de la LTrans. Quelle sera la situation sous l'empire de la nouvelle loi qui prévoit une obligation d'annonce ? Ne serait-il pas opportun d'introduire une limitation temporelle concernant l'accès à ce type d'information ?

Articles 27 ss P-OLPD

La disponibilité de ressources indépendantes pour tout organe fédéral est-elle objectivement acquise ? En pratique, quelles sanctions pourraient éventuellement être imposées au conseiller à la protection des données en cas de manquement, par qui au regard de l'indépendance qui lui est reconnue ? Par ailleurs, comment la fonction de conseiller à la protection des données s'intégrera-t-elle dans le cadre de la nouvelle loi sur la sécurité de l'information (LSI) ? A-t-on pré-examiné l'opportunité d'associer, même partiellement, cette fonction à celle de préposé-e à la sécurité de l'information ?

RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

Genève, le 13 octobre 2021

Le Conseil d'Etat

4863-2021

Département fédéral de Justice et Police
(DFJP)
Madame Karin Keller-Sutter
Conseillère fédérale
Palais fédéral Ouest
3003 Berne

Concerne : procédure de consultation fédérale sur le projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Madame la Conseillère fédérale,

Notre Conseil accuse bonne réception de la consultation mentionnée sous rubrique.

Nous avons procédé à un examen attentif du projet d'OLPD révisée et du rapport explicatif qui l'accompagne. La République et canton de Genève n'entre pas dans le champ d'application de la loi fédérale sur la protection des données, du 25 septembre 2020 (nLPD) ni de l'OLPD, qui visent le traitement de données personnelles de personnes physiques par les personnes privées ainsi que par les organes fédéraux. Notre Conseil souhaiterait toutefois vous faire part de quelques observations, respectivement, propositions.

Vous trouverez les points qui nous paraissent les plus importants ci-après. Pour le surplus, l'ensemble des remarques de notre Conseil figure dans le tableau que vous trouverez en annexe.

S'agissant des règlements de traitements automatisés (art. 4 P-OLPD), la nouvelle disposition nous paraît faire double emploi avec celle relative au registre des activités de traitement, déjà prévu par la nouvelle loi fédérale sur la protection des données, du 25 septembre 2020 (art. 12). La nouvelle teneur ne permet pas, à notre sens, de comprendre clairement son utilité par rapport au registre des activités de traitement, dont certaines indications se recoupent avec celles du règlement de traitements automatisés. Nous pensons donc que cette disposition devrait être précisée.

Par rapport à la communication de données à l'étranger (art. 8 P-OLPD), notre Conseil estime que le système d'une liste non exhaustive des Etats dont la législation assure un niveau de protection adéquat n'est pas satisfaisante, et que le système actuel d'une liste exhaustive doit être maintenu pour faciliter l'application de la loi – tout particulièrement par les personnes et entreprises privées – et les échanges avec l'étranger.

Enfin, en ce qui concerne l'exception à la gratuité en cas de communication de renseignements occasionnant des "efforts disproportionnés" (art. 23 P-OLPD), il nous semble, tout d'abord, que l'ordonnance devrait préciser la notion d' « efforts disproportionnés », qui est reprise de la loi. Par ailleurs, un émolument de 300 francs paraît

très insuffisant s'il est la rétribution d'un travail qui est qualifié, dans la même disposition, de disproportionné. Enfin, l'avant-projet d'OTrans, qui avait été mis en consultation par la Commission des institutions politiques du Conseil national, prévoit que lorsqu'une demande d'accès nécessite un surcroît important de travail de sa part, l'émolument pouvait s'élever à 2'000 francs au maximum. Notre Conseil considère donc que l'émolument ne devrait pas être plafonné ou alors, devrait être en tous les cas harmonisé avec l'avant-projet d'OTrans.

En vous remerciant de nous avoir consultés et de l'attention que vous porterez à la présente prise de position, nous vous prions de croire, Madame la Conseillère fédérale, à l'expression de notre parfaite considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Michèle Righetti

Le président :

Serge Dal Busco

Annexe mentionnée

Copie à : jonas.amstutz@bj.admin.ch

Annexe au courrier du Conseil d'Etat de la République et canton de Genève du 13 octobre 2021 à l'attention de Madame Karin Keller-Sutter, Conseillère fédérale, répondant à la consultation fédérale sur le projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

S'agissant du P-OLPD

Article	Commentaire
2, let i	Il nous semble que le terme « rapidement » est trop vague et ne tient pas assez compte du contexte. Le RGPD utilise les termes « délais appropriés ». Il nous semble que le délai devrait être approprié par rapport à l'usage attendu de la donnée et de la fréquence de sa consultation. **Nous proposons dès lors remplacer les termes "*peuvent être rapidement rétablis*" par "*peuvent être rétablis dans des délais appropriés*".**
3, al. 4	La notion de « procès-verbaux de journalisation » semble inconnue des spécialistes de la sécurité. Elle devrait être modifiée ou définie, afin de mieux cerner à quoi elle se rapporte. **En cas de modification, nous proposons de remplacer les termes *"procès-verbaux de journalisation"* par *"données de journalisation".*** Par ailleurs, au vu de la teneur de cette disposition, nous comprenons que seuls les auditeurs, le PFPDT et le conseiller à la protection des données pourront avoir accès aux « procès-verbaux de journalisation ». Or, il nous semble que les opérateurs des systèmes devraient aussi pouvoir y avoir accès, dans la mesure où ils pourraient en avoir besoin à des fins de support, par exemple. Nous pensons donc qu'il serait préférable que cette disposition soit reformulée. **Nous proposons de remplacer les termes *« organes ou personnes chargées de vérifier l'application des dispositions de protection des données personnelles ou de rétablir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données »* par « *« Ils sont accessibles aux seuls organes et personnes chargée de les exploiter ou d'effectuer des contrôles en matière de sécurité ».*** Enfin, il nous semble qu'une augmentation de la durée de conservation des « procès-verbaux de journalisation » d'un an à deux ans est trop importante, trop longue et potentiellement dangereuse (en cas de cyberattaque par exemple, les intrus pourraient aussi accéder aux logs sur une durée de deux ans). Il nous semble qu'une durée de 18 mois serait préférable tout en étant proportionnelle. **Nous proposons donc que cette disposition soit modifiée en ce sens. Si cette proposition devait être suivie, le délai de deux**

	ans devrait également être réduit à 18 mois dans toutes les ordonnances de l'Annexe 2 (Abrogation et modification d'autres actes) où ce délai figure.
4	La nouvelle disposition nous paraît faire doublon avec celle relative au registre des activités de traitement. La nouvelle teneur ne permet pas, à notre sens, de comprendre clairement son utilité par rapport au registre des activités des traitements. **Nous pensons donc que cette disposition devrait être précisée.**
8, al. 5	Le rapport explicatif précise que si un Etat ne figure pas dans la liste, cela ne signifie pas nécessairement qu'il soit dépourvu d'une législation sur la protection des données assurant un niveau de protection adéquat. Ce système n'est pas satisfaisant car il complexifie l'application de la loi et les échanges avec l'étranger. Les personnes ou les PME de droit privé n'auront en pratique pas les moyens de mener des recherches et analyses de droit international. **Nous pensons donc que le système d'une liste exhaustive des Etats dont la législation assure un niveau de protection adéquat (comme actuellement) serait préférable.**
9, al. 1 (en général)	Nous nous demandons dans quelle mesure il ne faudrait pas attirer l'attention des entreprises, au moins dans le rapport explicatif, sur les conséquences de l'arrêt Schrems II, qui rappelle qu'il appartient à l'exportateur des données (notamment le responsable de traitement) de veiller à l'établissement de garanties appropriées. Les clauses types consacrent uniquement des obligations contractuelles entre les parties au transfert, quel que soit le pays vers lequel les données sont transmises. Si le droit du pays de destination pose des risques particuliers (p. ex. s'agissant d'éventuelles ingérences des autorités locales), il appartient à l'exportateur de données d'adopter des mesures supplémentaires afin d'assurer un niveau de protection adéquat (voir consid. 109 RGPD). Ainsi, en vertu de cet arrêt, la seule convention de transmission de données ne suffit pas, mais les parties à la convention doivent s'assurer que les stipulations contenues dans ses clauses constituent un moyen suffisant permettant d'assurer, en pratique, la protection effective des données à caractère personnel transférées dans le pays tiers concerné (ie que le droit national ne s'y oppose pas ou ne les vide pas de leur sens).
9, al. 1 let. k, ch. 4	Même remarque que *supra* ad art. 9, al. 1 (en général).
19, al. 1	Nous pensons qu'il faudrait préciser le moment à partir duquel le délai d'annonce commence à courir, dans la mesure où la nLPD n'est pas assez précise sur ce point. **Nous proposons à cet égard d'indiquer que le délai commence à courir *« à partir de la découverte de la violation »*.**

19, al. 2	Nous pensons qu'il serait préférable d'harmoniser les termes utilisés dans la nLPD et le P-OLPD, par souci de cohérence et afin de ne pas étendre des délais qui sont déjà plus longs que ce que prévoit le RGPD. **Nous proposons donc de remplacer les termes *« sans retard excessif »* par les termes *« dans les meilleurs délais »*.**
22, al. 2	Afin de préserver au mieux les droits des personnes concernées, il nous semble important qu'un délai maximal soit fixé au responsable du traitement, pour éviter que les responsables de traitement fassent volontairement traîner les choses, en espérant que les personnes concernées abandonnent leurs prétentions. **Nous proposons donc que cette disposition soit précisée en ce sens.**
23, al. 1 *in fine*	La notion d'« efforts disproportionnés » reprend la notion prévue à l'art. 25, al. 6 LPD, sans pour autant la définir. Il serait utile de définir cette notion au niveau de l'ordonnance, ou de donner des exemples. L'émolument de 300 fr. paraît très insuffisant s'il est la rétribution d'un travail qui est qualifié, dans la même disposition, de disproportionné. Par ailleurs, l'avant-projet d'OTrans, qui avait été mis en consultation par la Commission des institutions politiques du Conseil national, prévoit que lorsqu'une demande d'accès nécessite un surcroît important de travail de sa part, l'émolument pouvait s'élever à 2'000 fr. au maximum. **Nous pensons donc que l'émolument ne devrait pas être plafonné ou alors, devrait en tous les cas être harmonisé avec l'avant-projet d'OTrans.**

S'agissant des modifications à d'autres actes

Acte	Commentaire
Ordonnance du 11 septembre 1996 sur le service civil (112)	Dans la version française du projet, il manque le verbe « gère » ou « tient » dans le texte de l'art. 110 al. 1 LSC (dans la version allemande : führt / dans la version italienne : gestisce)
Ordonnance du 6 juin 2014 concernant les systèmes d'information du service vétérinaire public (125)	Le vétérinaire cantonal souhaiterait que les demandes concernant les systèmes d'information du service vétérinaire public soient effectuées par écrit exclusivement. Il s'agirait ainsi de supprimer la seconde phrase de l'article 26 al. 2.

kanton glarus

Telefon 055 646 60 11/12/15
E-Mail: staatskanzlei@gl.ch
www.gl.ch

Regierungsrat
Rathaus
8750 Glarus

per E-Mail
jonas.amstutz@bj.admin.ch

Glarus, 5. Oktober 2021
Unsere Ref: 2021-203

Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Hochgeachtete Frau Bundesrätin
Sehr geehrte Damen und Herren

Das Eidgenössische Justiz- und Polizeidepartement (EJPD) gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und lassen uns gerne wie folgt vernehmen:

1. Grundsätzliche Einschätzung

Bei der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) handelt es sich um eine Ausführungsverordnung zum neuen Datenschutzgesetz (nDSG), welches vom Bundesparlament am 25. September 2020 totalrevidiert worden ist. Mit der nun vorgeschlagenen totalrevidierten VDSG soll das neue Gesetzesrecht auf Verordnungsstufe umgesetzt werden. Zentrale Regelungsinhalte bilden dabei die Neuregelung der Datensicherheit, der Bekanntgabe von Personendaten ins Ausland, der bisherigen Bestimmungen zum betrieblichen Datenschutzverantwortlichen, der Ausnahmen von der Registerführungspflicht und der Bestimmungen über den eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. Darüber hinaus enthält die totalrevidierte VDSG auch Bestimmungen zur Datenbearbeitung durch Auftragsbearbeiter, zur Informationspflicht, zur Meldung von Datenschutzverletzungen sowie zur Durchführung von Pilotversuchen.

Die Revision ist für den Kanton Glarus insoweit von Bedeutung, wie sie die allgemeinen Voraussetzungen und Grundsätze der Datenbearbeitung, vor allem aber auch die Bearbeitung von Personendaten durch Bundesorgane beschlägt. Dies mit Blick darauf, dass die Landsgemeinde am 5. September 2021 dem Erlass eines Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) zugestimmt hat. Mit Erlass des IDAG geht eine Totalrevision des kantonalen Datenschutzrechts einher, die ebenfalls eine Anpassung des dazugehörigen Verordnungsrechts verlangt. Auch wenn der Kanton Glarus formell nicht zur Übernahme des Bundesdatenschutzrechts verpflichtet ist, erscheint eine gewisse inhaltliche Harmonisierung der Regelungen auch auf Verordnungsebene sinnvoll. Der Regierungsrat unterstützt deshalb die nun in Angriff genommene Revision der VDSG in ihrer Stossrichtung. Dabei anerkennt er insbesondere den Handlungsbedarf, die Zielsetzung und die wesentlichen Regelungsinhalte. Gleichzeitig stellt sich für den Regierungsrat die Frage, ob mit den vorgeschlagenen Regelungen eine wirksame Umsetzung des neuen Daten-

schutzgesetzes erreicht werden kann. Er regt an, einzelne Bestimmungen und Regelungskonzepte nochmals zu überprüfen und gegebenenfalls anzupassen. Dabei orientiert er sich an der Stellungnahme der Konferenz der schweizerischen Datenschutzbeauftragten, Privatim, vom 1. September 2021.

2. Anmerkungen zu einzelnen Bestimmungen

2.1. Datensicherheit (Art. 1–5)

Artikel 1–5 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 nDSG). Dabei verlangt Artikel 8 Absatz 3 nDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt. Die Festlegung von Massnahmen für die Datensicherheit und deren Angemessenheit bedarf einer vorgängigen Beurteilung des *Schutzbedarfs*, der *Schutzziele* und der *Risiken* in Bezug auf die *Vertraulichkeit*, *Verfügbarkeit*, *Integrität* und *Nachvollziehbarkeit* von Personendaten und ihrer Bearbeitung. Dabei erscheint dem Regierungsrat eine Differenzierung nach *Sicherheitsstufen* sinnvoll, so wie dies bereits im Bundesgesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG; BBl 2020 9975) vorgesehen ist (vgl. Art. 17 ISG; Grundschutz – hoher Schutz – sehr hoher Schutz). Statt diesem neuen Ansatz zu folgen, hält der Entwurf am (veralteten) Konzept des geltenden Rechts fest. Nach Ansicht des Regierungsrates ist der 1. Abschnitt (Datensicherheit) des Verordnungsentwurfs deshalb konzeptionell grundlegend zu überarbeiten.

2.2. Artikel 2; Schutzziele

Die in Artikel 2 aufgeführten Vorgaben stellen keine eigenständigen Schutzziele dar, sondern Anforderungen an die Massnahmen, welche zur Erreichung der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit; vgl. auch Art. 6 Abs. 2 ISG) zu treffen sind. So stellt etwa die Zugriffskontrolle eine Anforderung zur Gewährleistung der Vertraulichkeit im Rahmen des Verhältnismässigkeitsprinzips dar, nicht jedoch ein Schutzziel.

Zudem ist der Einleitungssatz von Artikel 2 missverständlich. Schutzziele sind Zielvorgaben. Die Massnahmen müssen angemessen sein in Bezug auf die in der Risikobeurteilung festgestellten Risiken und nicht in Bezug auf die Schutzziele.

2.3. Artikel 3; Protokollierung

Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein durch Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und u.U. sanktioniert) werden kann. Die Pflicht zur Protokollierung stellt mitunter eine kompensatorische bzw. ergänzende Massnahme zur Gewährleistung der Datensicherheit dar.

Auch wenn es sich bei der Protokollierung selbst um eine Bearbeitung von Personendaten handelt, die sich am Verhältnismässigkeitsprinzip zu messen hat, begrüsst es der Regierungsrat, dass gemäss Absatz 2 für Bundesorgane und ihre Auftragsbearbeiter mit der Pflicht zur Protokollierung sämtlicher automatisierter Bearbeitungsvorgänge strengere Anforderungen an die Protokollierungspflicht gelten sollen als für private Verantwortliche und deren Auftragsbearbeiter nach Absatz 1. Nach Ansicht des Regierungsrates stärkt dies das Vertrauen in die Bearbeitung von Personendaten durch öffentliche Organe und wird durch die Protokollierungspflicht eine wirksame Kontrolle erst ermöglicht. Schliesslich dürfte der Protokollierungspflicht auch eine gewisse präventive Wirkung zukommen.

Um aber dem durchaus berechtigten Einwand, wonach eine Protokollierung jedes Lesezugriffs selbst bei einfachen Personendaten und bei restriktiven Berechtigungen unverhältnismässig wäre, Rechnung zu tragen, schlägt der Regierungsrat vor, die in Absatz 4 festgelegte

Aufbewahrungsdauer von zwei auf ein Jahr zu verkürzen. Dies in Anlehnung an bereits bestehende kantonale Regelungen wie z.B. diejenige des Kantons Aargau (vgl. § 5 Abs. 2^{bis} Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen vom 26. September 2007 [VIDAG; SAR 50.711]).

2.4. Artikel 7; Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans

Mit dem Erlass des IDAG hat die Landsgemeinde auch einer Änderung des EG StPO und des kantonalen Polizeigesetzes zugestimmt, wonach die Staatsanwaltschaft und die Kantonspolizei je einen Datenschutzberater zu bezeichnen haben. Aufgrund der Kleinheit der Verhältnisse im Kanton Glarus wurde hingegen auf eine Pflicht zur generellen Einführung von betrieblichen Datenschutzberatern für sämtliche öffentlichen Organe verzichtet. Umso wichtiger ist es, dass die Datenschutzberater bei der Staatsanwaltschaft und der Kantonspolizei bei der Anwendung der Datenschutzvorschriften in ihren Dienststellen aktiv mitwirken und damit auch die neu zu schaffende Fachstelle Datenschutz entlasten. Vor diesem Hintergrund ist nicht nachvollziehbar, wieso die Datenschutzberater der Bundesorgane gemäss dem Verordnungsentwurf erst nachträglich über den Abschluss eines Vertrages zur Übertragung eines Datenbearbeitungsvorganges an einen Dritten informiert werden müssen. Im Erläuternden Bericht wird ausdrücklich auf die mit der Auftragsbearbeitung einhergehenden erhöhten Risiken hingewiesen (s. S. 24). Gerade in solchen Fällen ist es wichtig, frühzeitig Fachpersonen für Datenschutz, wie sie die Datenschutzberater darstellen (s. Art. 28 Abs. 1 Bst. a E-VDSG), einzubeziehen. Die nachträgliche Information widerspricht dem präventiven und risikoorientierten Ansatz des nDSG. Auf die Bestimmung ist deshalb zu verzichten.

2.5. Bekanntgabe von Personendaten ins Ausland (Art. 8–13)

Nach dem totalrevidierten Bundesdatenschutzgesetz legt der Bundesrat neu fest, welche Staaten oder internationale Organisationen als Voraussetzung für die Bekanntgabe von Personendaten ins Ausland einen angemessenen Datenschutzstandard gewährleisten. Die Staaten werden im Anhang zur VDSG tabellarisch aufgeführt, die Verordnung selbst legt neu die Kriterien fest, welche der Bundesrat bei seinem Entscheid berücksichtigt (Art. 8 E-VDSG). Des Weiteren werden die in Artikel 16 Absatz 2 nDSG genannten weiteren Möglichkeiten zur Gewährleistung eines geeigneten Datenschutzes (z.B. Standarddatenschutzklauseln) in der Verordnung inhaltlich konkretisiert (Art. 9 ff. E-VDSG). Schliesslich soll von der Delegation in Artikel 16 Absatz 3 nDSG, wonach andere geeignete Garantien vorgesehen werden können, Gebrauch gemacht werden. So dürfen ebenfalls Personendaten bekanntgegeben werden, wenn das angemessene Datenschutzniveau durch einen Verhaltenskodex oder eine Zertifizierung gewährleistet wird (Art. 12 E-VDSG).

Der Regierungsrat begrüsst diese Regelungen, an denen sich künftig auch das kantonale Datenschutzrecht für die Bekanntgabe von Daten ins Ausland durch kantonale öffentliche Organe orientieren kann. Insbesondere begrüsst er es, dass bei den Kriterien für den Angemessenheitsentscheid in Artikel 8 Absatz 1 neben den eigentlichen datenschutzrechtlichen Kriterien auch das allgemeine Kriterium «Achtung der Menschenrechte» Aufnahme gefunden hat. Zudem begrüsst der Regierungsrat, dass in Artikel 8 Absatz 1 eine Differenzierung nach «Staat», «Gebiet» oder «spezifische Sektoren in einem Staat» vorgenommen wird. Dies erlaubt es dem Bundesrat, bei seinem Angemessenheitsentscheid auf die örtlichen Verhältnisse Rücksicht zu nehmen, insbesondere auf die Gesetzgebung in einzelnen Gliedstaaten von Bundesstaaten wie der USA oder Kanada.

2.6. Artikel 20; Modalitäten (des Auskunftsrechts)

Das Abstellen auf die individuellen Fähigkeiten der um Auskunft ersuchenden Person bei der Aufbereitung der gewünschten Auskunft über die Bearbeitung eigener Personendaten in Absatz 3 schiesst über das Ziel hinaus. Der Inhalt der Auskunft ist in Artikel 25 Absatz 2 nDSG

definiert. Daraus ergeben sich der Umfang und der Zweck der Auskunft. Artikel 20 Absatz 3 ist ersatzlos zu streichen.

Wird das Auskunftsrecht durch ein Bundesorgan eingeschränkt bzw. gar gänzlich verweigert, so ist dies gegenüber der betroffenen Person zu verfügen. Die Gründe für die Einschränkung sind in der Verfügung auszuführen, die Dokumentations- und Aufbewahrungspflicht ergibt sich aus der verfahrensrechtlichen Aktenführungspflicht. Vor diesem Hintergrund erübrigt sich eine spezielle Regelung in Artikel 20 Absatz 5. Die Bestimmung ist ersatzlos zu streichen.

2.7. Artikel 21; Zuständigkeit (für die Erteilung der Auskunft)

Absatz 1 sieht vor, dass ein Verantwortlicher, der für die Behandlung des Begehrens nicht zuständig ist, dieses an den zuständigen Verantwortlichen weiterleitet. Dieser verwaltungsrechtliche Grundsatz gilt für die Bundesorgane auch ohne Erwähnung in diesem Zusammenhang. Die Bestimmung (Art. 21 Abs. 1 Satz 2 E-VDSG) ist ersatzlos zu streichen. Ebenfalls zu streichen ist Absatz 2, ist es doch Aufgabe des Verantwortlichen die für die Auskunftserteilung notwendigen Informationen beim Auftragsbearbeiter einzuholen und über das Auskunftsbegehren zu entscheiden.

Genehmigen Sie, hochgeachtete Frau Bundesrätin, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Für den Regierungsrat

Marianne Lienhard
Landammann

Hansjörg Dürst
Ratsschreiber

E-Mail an (PDF- und Word-Version):
- jonas.amstutz@bj.admin.ch

Die Regierung
des Kantons Graubünden

La Regenza
dal chantun Grischun

Il Governo
del Cantone dei Grigioni

Sitzung vom	Mitgeteilt den	Protokoll Nr.
12. Oktober 2021	14. Oktober 2021	894/2021

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Per E-Mail (PDF- und Word-Version) zustellen an: jonas.amstutz@bj.admin.ch

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Juni 2021 erhalten die Kantone Gelegenheit, sich zu erwähntem Geschäft zu äussern. Dafür danken wir Ihnen bestens.

Die uns zugesandte Dokumentation haben wir geprüft. Die Regierung erachtet den nun vorliegenden Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) als noch überarbeitungsbedürftig. Er schafft in der vorliegenden Version noch zu wenig Klarheit für die Umsetzung durch die Verantwortlichen. Einerseits liegt das daran, dass überholte Begriffe und Bestimmungen der bisherigen Verordnung übernommen werden. Andererseits erreichen die neuen Bestimmungen nicht die für die Umsetzung des an sich schon komplexen neuen Datenschutzgesetzes (nDSG) notwendige Detaillierung. Folgerichtig sollen sämtliche Bestimmungen auf die konsequente Umsetzung des nDSG ausgerichtet sein. Für die Details verweisen wir auf die nachfolgenden Ausführungen zu den einzelnen Artikeln des Entwurfs.

1. Bemerkungen zu einzelnen Artikeln

Art. 1 bis 4 E-VDSG

Die Bestimmungen über die Datensicherheit orientieren sich am veralteten Konzept der bisherigen Verordnungen und ergänzen diese mit Bestimmungen aus dem europäischen Recht. Im Bereich Datensicherheit geht es um die Konkretisierung von Art. 8 nDSG. Im Zusammenhang mit der Verabschiedung des Bundesgesetzes über die Informationssicherheit (ISG) hat der Bund eine moderne Umsetzung aufgezeigt. Daran sollte sich der Gesetzgeber orientieren und die Bestimmungen von Art. 1 bis 4 E-VDSG konzeptionell überarbeiten.

Art. 2 E-VDSG

Die Aufzählungen in Art. 2 E-VDSG haben abschliessenden Charakter. In Anbetracht der sich stetig und relativ schnell ändernden Rahmenbedingungen ist eine allgemeine Formulierung angezeigt. Jedenfalls muss ein Hinweis auf eine nicht abschliessende Aufzählung erfolgen (bspw. "insbesondere"), um den stetigen Änderungen Rechnung zu tragen.

Art. 3 E-VDSG

Insbesondere für Bundesorgane sieht Art. 3 E-VDSG eine ausführliche Protokollierung der Datenbearbeitung vor.

Die Protokollierung hat den Zweck, dass in Situationen, in denen ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt werden kann. Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit dem Blick auf ein konkretes Risiko sein, dass mittels Protokollierung wirksam reduziert werden kann. Dass ein irgendwie geartetes Risiko verbleibt, reicht nicht. Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen umfassende Berechtigungen implementiert werden müssen, weil nicht zum vornherein bekannt ist, auf welche konkreten Daten eine berechtigte Person bei der Aufgabenerfüllung Zugang haben muss. Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert

und stichprobenweise überprüft werden. Die Pflicht zur Protokollierung als kompensierende Massnahme ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert.

Für die Bundesorgane soll die Protokollierung für das Bearbeiten sämtlicher Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Dies geht deutlich zu weit. Die Protokollierung stellt selbst eine Beschaffung von Personendaten dar, die dem Grundsatz der Verhältnismässigkeit genügen muss. Da selbst bei einfachen Personendaten und bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht klar über dessen Anforderung hinaus. Die Bundesorgane sind deshalb in Art. 3 Abs. 1 E-VDSG aufzunehmen und auf Art. 3 Abs. 2 E-VDSG ist zu verzichten.

Art. 4 E-VDSG

Die Erstellung eines Bearbeitungsreglements wird für private Verantwortliche und deren Auftragsbearbeitende vorgesehen, die umfangreich besonders schützenswerte Personendaten bearbeiten oder ein Profiling mit hohem Risiko durchführen (Art. 4 Abs. 1 E-VDSG). Diese Eingrenzung erscheint willkürlich und deckt bei weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen ab.

Hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen. Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt, die Teil des Bearbeitungsreglements sein können.

Art. 19 E-VDSG

Art. 24 Abs. 1 nDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führen. Art. 24 Abs. 2 nDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzung für die Informationen der betroffenen Personen (Art. 24 Abs. 4 und 5 nDSG).

Art. 20 E-VDSG

Das Auskunftsrecht und dessen Einschränkungen regeln Art. 25 nDSG und Art. 26 nDSG ausführlich. Art. 20 E-VDSG bringt hierzu einige Konkretisierungen, die aber über das Notwendige hinausgehen.

Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 nDSG definiert. Daraus ergeben sich der Umfang und der Zweck der Auskunft. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechtes in die Prozesse der Verantwortlichen integriert werden könnte. Demzufolge ist Art. 20 Abs. 3 E-VDSG ersatzlos zu streichen.

Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, "die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen". Dies ergibt sich bereits aus Art. 8 nDSG und den Bestimmungen des ersten Artikels der E-VDSG. Diese Erwähnung ist in Art. 20 Abs. 4 E-VDSG zu streichen.

Art. 26 Abs. 4 nDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person um ihren Auskunftsanspruch allenfalls gerichtlich überprüfen zu lassen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechtes durch die betroffene Person. Art. 20 Abs. 5 E-VDSG ist ersatzlos zu streichen.

Art. 25 E-VDSG

Die Aufgaben, die die Datenschutzberaterin oder der Datenschutzberater wahrnehmen muss, sind in Art. 25 E-VDSG festgehalten. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 nDSG, der namentlich zwei Aufgaben aufzählt, nämlich die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Buchstabe a und b E-VDSG nicht die Aufgaben sind, die sie oder er wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 nDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 2 E-VDSG ist missverständlich und zu korrigieren.

Art. 26 E-VDSG

In Anwendung von Art. 12 Abs. 5 nDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn umfangreich besonders schützenswerte Personendaten bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird. Wie bereits unter Art. 4 Abs. 1 E-VDSG erwähnt wurde, deckt diese Eingrenzung bei weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen ab. Auch hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen.

Art. 36 E-VDSG

Diese Bestimmung ist überflüssig, weil sich diese Präzisierung bereits aus Art. 39 nDSG klar ergibt.

2. Kontaktpersonen

Gemäss Schreiben vom 21. März 2021 wird im Hinblick auf allfällige Rückfragen die Angabe von Kontaktpersonen gewünscht. Es handelt sich um:
Frau Dr. iur. Regula Hunger (Departementssekretärin, Departement für Justiz, Sicherheit und Gesundheit; Tel. 081 257 25 13; Regula.Hunger@djsg.gr.ch).

Abschliessend danken wir Ihnen für die Berücksichtigung unserer Anliegen.

Namens der Regierung

Der Präsident:	Der Kanzleidirektor:
Dr. Mario Cavigelli	Daniel Spadin

KANTON LUZERN

Justiz- und Sicherheitsdepartement
Bahnhofstrasse 15
Postfach 3768
6002 Luzern
Telefon 041 228 59 17
justiz@lu.ch
www.lu.ch

Eidgenössisches Justiz- und Polizeidepartement

per E-Mail
jonas.amstutz@bj.admin.ch

Luzern, 28. September 2021

Protokoll-Nr.: 1142

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Juni 2021 haben Sie die Kantonsregierungen und interessierte Organisationen zur Stellungnahme zum VDSG-Entwurf eingeladen.

Im Namen und Auftrag des Regierungsrates teilen wir Ihnen mit, dass der Kanton Luzern mit dem vorgeschlagenen Verordnungsentwurf grundsätzlich einverstanden ist. Das eidgenössische Datenschutzrecht regelt die Datenbearbeitung durch Private und die Bundesorgane. Der Kanton Luzern hat seine geänderten Datenschutzerlasse bereits auf den 1. September 2021 in Kraft gesetzt (vgl. Gesetzessammlung vom 28. August 2021).

Zu einzelnen Bestimmungen des VDSG-Entwurfes haben wir im Hinblick auf die privaten Personen, mithin die Regelungen für die Unternehmen der Wirtschaft, Vorbehalte. Insbesondere Artikel 4 betreffend das Obligatorium für Bearbeitungsreglemente sollte im Hinblick auf die ausreichende Gesetzesgrundlage näher geprüft werden. Das Gesetz gibt dem Bundesrat lediglich die Kompetenz, Bestimmungen über die Mindestanforderungen an die *Datensicherheit* zu erlassen (Art. 8 Abs. 3 revDSG) und verlangt von den Verantwortlichen ein Verzeichnis der Bearbeitungstätigkeiten (Art. 12 revDSG). Artikel 1 und 2 VDSG-Entwurf lassen dementsprechend die technischen und organisatorischen Massnahmen, die Unternehmen und andere privatrechtliche Organisationen zu ergreifen haben, zu Recht offen und geben lediglich Kriterien und Schutzziele vor. Wird das Erlassen von Bearbeitungsreglementen als zulässige Mindestanforderung der Datensicherheit im Sinn der Gesetzesbestimmung aufgefasst, was zweifelhaft erscheint, muss darauf hingewiesen werden, dass die Verletzung von Mindestanforderungen gemäss Artikel 61 revDSG mit Busse bestraft wird, wozu sich aber der unbestimmte Tatbestand (u.a. «umfangreich besonders schützenswerte Personendaten bearbeiten») nicht eignet. Das Verhältnis der Bestimmungen des ersten Abschnittes der Verordnung – Grundsätze, Schutzziele, Protokollierung (in Abhängigkeit von Datenschutz-Folgenabschätzung), Bearbeitungsreglement – zu dieser Strafbarkeitsnorm ist im Interesse der Rechtssicherheit vertieft zu klären.

Dem erläuternden Bericht zu Artikel 6 Absatz 3 über die Übertragung der Datenbearbeitung an weitere Auftragsbearbeiter ist zur Wendung «schriftlich genehmigt» zu entnehmen, dass die elektronische Form eingeschlossen ist. Da in der rechtswissenschaftlichen Lehre Uneinigkeit darüber besteht, ob unter dem Begriff «schriftlich» auch die «elektronische Form» zu verstehen ist, regen wir an, diese und weitere Bestimmungen hinsichtlich der Handlungsformen zu überprüfen. Entweder könnte die elektronische Form ausdrücklich erwähnt werden oder als technikneutrale Alternative Wendungen wie «ausdrückliche Zustimmung» oder «in Textform festlegen» oder «aufzeichnen» verwendet werden, sofern die Streichung der Formvorschriften nicht ohnehin angebracht ist. Neben den expliziten Formvorschriften stellen wir auch einige der in der Verordnung enthaltenen Dokumentations- und (mit unterschiedlichen Zeitdauern versehenen) Aufbewahrungspflichten in Frage (insbes. diejenige von Art. 20 Abs. 5, für die es keine gesetzliche Grundlage gibt). Im Sinn einer Regulierungsfolgenvermeidung sollten solche Detailvorschriften überprüft werden.

Zu Artikel 13 und 15 über die Informationspflichten des Auftragsbearbeiters regen wir ebenfalls die Überprüfung im Hinblick auf eine ausreichende Gesetzesgrundlage an. Gemäss Artikel 19 revDSG obliegt die Informationspflicht gegenüber der betroffenen Person lediglich dem Verantwortlichen. Zudem umfassen die Informationspflichten laut Gesetz nicht die in Artikel 15 VDSG-Entwurf aufgeführten Punkte «Aktualität, Zuverlässigkeit und Vollständigkeit» der Personendaten und die im Entwurf genannten, von der Bekanntgabe dispensierenden Umstände sind unklar.

Problematisch ist auch Artikel 17 über die Überprüfung automatisierter Einzelentscheidungen. Das Gesetz regelt die Ansprüche der von solchen Entscheidformen betroffenen Personen (vgl. Art. 21 revDSG). Weiterungen sind auf Verordnungsstufe überflüssig beziehungsweise ihre Gesetzeskonformität wird in Frage gestellt, zumal das Gesetz mit Artikel 61 eine Strafbarkeitsbestimmung vorsieht.

Gemäss Artikel 10 revDSG können private Verantwortliche einen Datenschutzberater oder eine -beraterin als Anlaufstelle für Datenschutzfragen ernennen. Die in Artikel 25 VDSG-Entwurf verwendeten Muss-Formulierungen bei den Pflichten überzeugen daher nicht, wenn der Berater für die Privaten freiwillig ist. Zudem widerspricht die Prüfpflicht jeglicher Datenbearbeitung (Abs. 1 lit. a) dem in Artikel 8 revDSG enthaltenen risikobasierten Ansatz.

Artikel 26 über die Ausnahmeregelung für Unternehmen mit weniger als 250 Mitarbeitende begrüssen wir als Handlungsoption für Private. Das in Buchstabe b angeführte Risiko sollte der Klarheit halber ergänzt werden mit der Formulierung «für die Persönlichkeit oder die Grundrechte der betroffenen Personen» (dies analog Art. 3 Abs. 1).

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Paul Winiker
Regierungsrat

LE CONSEIL D'ÉTAT
DE LA RÉPUBLIQUE ET
CANTON DE NEUCHÂTEL

Département fédéral de justice et police
Palais fédéral
3001 Berne

Projet de révision totale de l'ordonnance fédérale relative à la protection des données (OLPD)

Madame la conseillère fédérale,

Le Conseil d'État de la République et Canton de Neuchâtel a pris connaissance avec intérêt du projet mentionné en rubrique.

Dans la mesure où le projet ne concerne pas les cantons, seules les personnes privées et les organes fédéraux entrant dans le champ d'application de la LPD et par conséquence du projet d'OLPD, le gouvernement neuchâtelois n'a pas de remarque à formuler.

En vous remerciant de nous avoir consultés, nous vous prions de croire, Madame la conseillère fédérale, à l'assurance de notre parfaite considération.

Neuchâtel, le 15 septembre 2021

Au nom du Conseil d'État :

Le président,
L. FAVRE

La chancelière,
S. DESPLAND

RÉPUBLIQUE ET CANTON DE NEUCHÂTEL * CONSEIL D'ÉTAT *

KANTON NIDWALDEN
LANDAMMANN UND REGIERUNGSRAT
Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

CH-6371 Stans, Dorfplatz 2, Postfach 1246, STK

PER E-MAIL
Eidg. Justiz- und Polizeidepartement (EJPD)
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 28. September 2021

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz; Stellungnahme

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Juni 2021 eröffnete das Eidgenössische Justiz- und Polizeidepartement (EJPD) das Vernehmlassungsverfahren zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG). Für die Möglichkeit Stellung nehmen zu können, danken wir bestens.

Das revidierte Bundesgesetz über den Datenschutz vom 25. September 2020 (rDSG) beinhaltet zahlreiche Delegationsnormen, auf die sich der vorliegende Entwurf der VDSG (nachfolgend E-VDSG) stützt. Zudem konkretisiert der E-VDSG verschiedene Bestimmungen des rDSG. Wir begrüssen den vorliegenden Entwurf. Es entsteht aber der Eindruck, dass die Verordnung bei einzelnen Bestimmungen zu wenig Klarheit für die Umsetzung durch die Verantwortlichen schafft. Einerseits liegt dies darin, dass überholte Begriffe und Bestimmungen der bisherigen Verordnung einfach übernommen werden. Andererseits bringen die neuen Bestimmungen kaum die notwendige Detaillierung für die Umsetzung des an sich schon komplexen rDSG. So werden die Verantwortlichen (private Personen wie auch Bundesorgane) wohl Mühe haben, verschiedene dieser Bestimmungen angemessen umzusetzen. Wir empfehlen daher, gewisse Bestimmungen im Hinblick auf eine wirkungsvolle Umsetzung des Datenschutzes zu überprüfen.

Zu Art. 1 - 4 E-VDSG (Datensicherheit)

Die Art. 1 bis 4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 rDSG). Dabei verlangt Art. 8 Abs. 3 rDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt.
Der E-VDSG hält am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht, ohne aber Art. 8 rDSG für die Praxis zu konkretisieren. Eine solche Konkretisierung wäre aber gerade für die verantwortlichen öffentlichen Organe (also Bundesorgane) und Private sehr wichtig und entscheidend. Denn sie müssen erkennen können, was sie im Bereich der Datensicherheit tun müssen und wie dies erfolgen könnte (z.B. anhand von Leitlinien).

Zu Art. 1 E-VDSG

Aus Art. 1 Abs. 1 E-VDSG ergibt sich, dass die Angemessenheit von Massnahmen sich nach den Kriterien Zweck, Art, Umfang und Umstände der Datenbearbeitung, Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen, Stand der Technik und Implementierungskosten beurteilt. Dabei sagen die für die Beurteilung der Angemessenheit der Massnahmen bestehenden Kriterien «Stand der Technik und Implementierungskosten» wohl nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche dem Risiko mit der nötigen Effektivität begegnet. Dies wird beispielsweise auch in Art. 32 DSGVO so geregelt.

Art. 1 Abs. 2 E-VDSG verlangt, dass die Massnahmen über die gesamte Bearbeitungszeit in angemessenen Abständen zu überprüfen sind. Diese Formulierung greift zu kurz. In erster Linie ist die Risikobeurteilung laufend zu überprüfen, woraus sich die Massnahmen und deren Angemessenheit ergeben und somit die allfällige Anpassung von Massnahmen. Zentral ist nämlich, dass einmal getroffene Massnahmen nicht per se weiterbestehen müssen, sondern dass dies ein kontinuierlicher Prozess darstellt, bei dem die Risiken immer wieder von neuem betrachtet, eingeordnet und dagegen entsprechende Massnahmen getroffen werden müssen.

Zu Art. 2 E-VDSG

Wir regen an, die in dieser Bestimmung beschriebenen Schutzziele, die bereits in Art. 5 Abs. 1 Bst. h rDSG angelegt sind, angepasst an den aktuellen Stand der Technik und in einer verständlichen Weise umzuformulieren. Mögliche diesbezügliche Formulierungen finden sich in § des Informations- und Datenschutzgesetzes des Kantons Basel-Stadt oder § 7 des Informations- und Datenschutzgesetzes des Kantons Zürich.

Zu Art. 3 E-VDSG

Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und dann unter Umständen sanktioniert) werden kann.
Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das mittels Protokollierung wirksam reduziert werden kann; dass ein irgendwie geartetes Risiko verbleibt, reicht nicht (es fehlt dann an der Verhältnismässigkeit der neuen Datenbearbeitung). Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen offene Berechtigungen implementiert werden müssen, weil nicht zum Vorherein bekannt ist, auf welche konkreten Daten der/die Berechtigte bei der Aufgabenerfüllung Zugang haben muss (z.B. im Schengen-Informationssystem). Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert und stichprobenweise überprüft werden. Die Pflicht zur Protokollierung ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert.

Für die Bundesorgane soll die Protokollierung für das Bearbeiten sämtlicher Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Das geht unseres Erachtens zu weit. Denn festzuhalten ist, dass die Protokollierung selbst eine Beschaffung von Personendaten darstellt, die somit dem Grundsatz der Verhältnismässigkeit genügen muss. Zwar erlaubt Art. 57l Bst. b Ziff. 4 RVOG die Aufzeichnung von Randdaten zum Nachvollzug des Zugriffs auf Datensammlungen, aber eben nur insoweit, als die Aufzeichnung verhältnismässig ist. Dass selbst bei einfachen Personendaten und selbst bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht über diese Anforderung hinaus. Es ist nicht klar eruierbar, warum die Pflicht der

Bundesorgane zur Protokollierung weitergehen soll als jene der privaten Verantwortlichen. Diese Thematik soll entsprechend nochmals angeschaut werden.

In Art. 3 Abs. 3 E-VDSG sollte vor «die Identität der Empfängerin oder des Empfängers» das Wort «gegebenenfalls» eingefügt werden, da es sich nicht bei jeder protokollierten Bearbeitung um eine Bekanntgabe handelt (sondern teilweise auch «nur» Abfragen getätigt werden, ohne dass Personendaten bekannt gegeben werden).

Gemäss Art. 3 Abs. 4 E-VDSG sind die Protokolle während zwei Jahren aufzubewahren und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei und dafür ist nicht in jedem Fall eine personenbezogene Auswertung erforderlich. Für die Bundesorgane legen die Art. 57m ff. RVOG und Art. 8 ff. der zugehörigen Ausführungsverordnung fest, wie die Auswertungen erfolgen dürfen, wobei ggf. auch ein gestaffeltes Vorgehen angezeigt ist (vgl. BGE 143 II 443). Der letzte Satz ist deshalb im Sinne «dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden» zu ergänzen.

Zu Art. 4 und 5 E-VDSG

Wir empfehlen, anstelle der zwei in Art. 4 Abs. 1 E-VDSG festgehaltenen alternativen Vorgaben die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 rDSG). Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 rDSG), die Teil des Bearbeitungsreglements sein können.

Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater (DB) ist die Fachperson. Ein Bearbeitungsreglement wird zusammen mit ihr erstellt und nicht «der DB in einer für diese verständlichen Form zur Verfügung» gestellt. Es gehört zu den Aufgaben der DB, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b rDSG). Weiter muss die DB über die erforderlichen Fachkenntnisse verfügen (Art. 10 Abs. 3 Bst. c rDSG), was mit der Formulierung, das Bearbeitungsreglement sei ihr «in verständlicher Form» zur Verfügung zu stellen, nicht vereinbar ist, weil letzteres eine Abwertung der Fachkompetenzen impliziert.

Diese Ausführungen gelten analog auch für Art. 5 E-VDSG.

Zu Art. 7 E-VDSG

Auch die DB des Bundesorgans hat bei der Anwendung der Datenschutzvorschriften mitzuwirken (vgl. unten Art. 28 E-VDSG). Es widerspricht dem präventiven und risikoorientierten Ansatz des rDSG, wenn die DB lediglich nachträglich über den Abschluss eines Outsourcingvertrags oder bei einer Funktionsübertragung informiert werden soll. Zu den Aufgaben der DB gehört die Involvierung in solche Geschäfte. Dies ist eine Kernaufgabe der DB als Beratungsfunktion («Mitwirkung bei der Anwendung der Datenschutzvorschriften»). Die DB ist rechtzeitig zu informieren (und «mit ins Boot zu holen»), wie dies korrekterweise bei Datenbearbeitungsprojekten vorgesehen ist (Art. 31 E-VDSG). Um Kompetenz- und Umsetzungsfragen (vor allem auch der Praxis) bereits im Voraus verhindern zu können, raten wir Ihnen, diese Bestimmung und darin vor allem die Position der DB entsprechend der Definition im rDSG zu stärken.

Zu Art. 8 E-VDSG

Bei den Formulierungen in dieser Bestimmung fällt auf, dass der EDÖB (formell) konsultiert wird und die Beurteilungen von internationalen Organisationen oder ausländischen Behörden berücksichtigt werden können (materiell). Es ist klar zu formulieren, dass auch die Stellungnahmen des EDÖB materiell zu berücksichtigen sind, zumal sich die Erläuterungen hierzu nicht äussern (Erläuterungen, S. 27).

Zu Art. 9 Abs. 3 E-VDSG

Gemäss Art. 16 Abs. 2 Bst. b und c rDSG sind Datenschutzklauseln und spezifische Garantien dem EDÖB vorgängig mitzuteilen. Der Einleitungssatz von Art. 9 Abs. 3 E-VDSG suggeriert, dass es einen Sachverhalt geben könnte, in der auch die Nicht-Mitteilung zu einer rechtskonformen Bekanntgabe ins Ausland führen würde. Wir empfehlen, diese Formulierung entsprechend anzupassen.

Zu Art. 19 E-VDSG

Art. 24 Abs. 1 rDSG sieht eine Meldung von Verletzungen der Datensicherheit in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 rDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 rDSG). Art. 24 rDSG ist eine (bewusst) abweichende Bestimmung von Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO aufgenommen. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen. Für die Mehrheit der Verantwortlichen trifft dies aber nicht zu. Art. 19 E-VDSG bringt somit unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht (die in der Praxis zudem möglichst rasch erfolgen soll) wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde rasch informiert wird, allenfalls auch die betroffenen Personen, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden. Es erscheint also fraglich, ob Art. 24 rDSG die in Art. 19 E- VDSG enthaltene Konkretisierung überhaupt braucht.

Zu Art. 20 E-VDSG

Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 rDSG definiert. Daraus ergeben sich Umfang und Zweck der Auskunft, was sich nach objektiven Kriterien misst. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte. Wir regen deshalb dazu an, Art. 20 Abs. 3 E-VDSG zu streichen.

Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen». Dies ergibt sich bereits aus Art. 8 rDSG und den Bestimmungen des 1. Kapitels der E-VDSG, weshalb diese Bestimmung gestrichen werden kann und soll.

Art. 26 Abs. 4 rDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an den Ver-

antwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person. Deshalb ist Art. 20 Abs. 5 E-VDSG ersatzlos zu streichen.

Zu Art. 25 E-VDSG

Art. 25 E-VDSG hält fest, welche Aufgaben die DB wahrnehmen muss. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 rDSG, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die er oder sie wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 rDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist missverständlich und entsprechend anzupassen. Dies könnte eventuell bereits mit dem Einfügen eines Passus wie «insbesondere» an geeigneter Stelle umgesetzt werden.

Zu Art. 26 E-VDSG

In Anwendung von Art. 12 Abs. 5 rDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn (1) umfangreich besonders schützenswerte Personendaten bearbeitet werden oder (2) ein Profiling mit hohem Risiko durchgeführt wird. Wie bei Art. 4 Abs. 1 E-VDSG ist zu erwähnen, dass diese Eingrenzung nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es unseres Erachtens angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 rDSG).

Zu Art. 36 E-VDSG

Diese Bestimmung ist überflüssig, weil sich die darin enthaltene Präzisierung bereits aus Art. 39 rDSG ergibt.

Wir hoffen, Ihnen mit diesen Angaben zu dienen, und bedanken uns für die Berücksichtigung unserer Hinweise.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES

Karin Kayser-Frutschi
Landammann

lic. iur. Armin Eberli
Landschreiber

Geht an:
- jonas.amstutz@bj.admin.ch

Kanton
Obwalden

Der Vorsteher des Sicherheits- und Justizdepartements SJD

CH-6061 Sarnen, Postfach 1561, SJD

Per E-Mail an:

Eidgenössisches Justiz
und Polizeidepartement EJPD
3003 Bern

jonas.amstutz@bj.admin.ch

Referenz/Aktenzeichen: OWSTK.4113
Unser Zeichen: fu

Sarnen, 13. Oktober 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Stellungnahme

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Für die Gelegenheit der Stellungnahme zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) danken wir Ihnen.

Wir stellen Ihnen im Anhang die Stellungnahme unseres Datenschutzbeauftragten vom 13. September 2021 zu und bitten Sie gewisse Bestimmungen im Hinblick auf eine wirkungsvolle Umsetzung des Datenschutzes bei gleichzeitiger Bedienerfreundlichkeit grundsätzlich zu überprüfen.

Wir danken Ihnen, sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, für die Berücksichtigung unserer Ausführungen.

Freundliche Grüsse

Christoph Amstad
Regierungsrat

Stellungnahme Datenschutzbeauftragter Schwyz, Ob- und Nidwalden vom 13.09.2021

Sicherheits- und Justizdepartement SJD
Postfach 1561, 6061 Sarnen
Tel. 041 666 62 19
sjd@ow.ch
www.ow.ch

Kopie an:
- Kantonale Mitglieder der Bundesversammlung
- Datenschutzbeauftragter Schwyz, Ob- und Nidwalden
- Amt für Justiz
- Kantonspolizei
- Staatskanzlei (Kommunikation)

DATENSCHUTZBEAUFTRAGTER
Schwyz - Obwalden - Nidwalden

Gotthardstrasse 21
6414 Oberarth

Datenschutz

Sicherheitsdepartement Kanton Schwyz
(Departementssekretariat)
Sicherheits- und Justizdepartement Kanton Obwalden
(Departementssekretariat)
Staatskanzlei Kanton Nidwalden
(Rechtsdienst)
(per E-Mail)

Oberarth, 13. September 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz: unsere Stellungnahme

Sehr geehrte Damen und Herren

Für die Möglichkeit, im Rahmen des Mitberichtsverfahrens zur totalrevidierten Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellung nehmen zu können, danken wir bestens. Gerne teilen wir Ihnen mit, dass sich aus datenschutzrechtlicher Sicht dazu folgende Bemerkungen ergeben:

1. Allgemeines

Das revidierte Bundesgesetz über den Datenschutz vom 25.09.2020 (rDSG) beinhaltet zahlreiche Delegationsnormen, auf die sich der vorliegende Entwurf der VDSG (nachfolgend E-VDSG) stützt (siehe Ingress E-VDSG). Zudem konkretisiert der E-VDSG verschiedene Bestimmungen des rDSG.

Insgesamt entsteht bisweilen der Eindruck einer Verordnung, die zu wenig Klarheit für die Umsetzung durch die Verantwortlichen schafft. Einerseits liegt es darin, dass überholte Begriffe und Bestimmungen der bisherigen Verordnung einfach übernommen werden. Andererseits bringen die neuen Bestimmungen kaum die notwendige Detaillierung für die Umsetzung des an sich schon komplexen rDSG. So werden die Verantwortlichen (private Personen wie auch Bundesorgane) wohl Mühe haben, verschiedene dieser Bestimmungen angemessen umzusetzen. Gerade eine angemessene Umsetzung der Vorgaben (sowohl des rDSG wie auch der E-VDSG) in der Praxis ist aber sehr wichtig; nicht zuletzt auch aufgrund der Tatsache, dass diese Vorgaben andernfalls nicht oder nur teilweise angewendet werden.

Dazu empfehlen wir, gewisse Bestimmungen im Hinblick auf eine wirkungsvolle Umsetzung des Datenschutzes grundsätzlich zu überprüfen.

2. Zu Art. 1 - 4 E-VDSG (Datensicherheit)

Die Art. 1 bis 4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 rDSG). Dabei verlangt Art. 8 Abs. 3 rDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt.

Der E-VDSG hält am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht, ohne aber Art. 8 rDSG für die Praxis zu konkretisieren. Eine solche Konkretisierung wäre aber gerade für die verantwortlichen öffentlichen Organe (also Bundesorgane) und Private sehr wichtig und entscheidend. Denn sie müssen erkennen können, was sie im Bereich der Datensicherheit tun müssen und wie dies erfolgen könnte (z.B. anhand von Leitlinien).

3. Zu Art. 1 E-VDSG

Aus Art. 1 Abs. 1 E-VDSG ergibt sich, dass die Angemessenheit von Massnahmen sich nach den Kriterien Zweck, Art, Umfang und Umstände der Datenbearbeitung, Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen, Stand der Technik und Implementierungskosten beurteilt. Dabei sagen die für die Beurteilung der Angemessenheit der Massnahmen bestehenden Kriterien «Stand der Technik und Implementierungskosten» wohl nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche dem Risiko mit der nötigen Effektivität begegnet. Dies wird beispielsweise auch in Art. 32 DSGVO so geregelt.

Art. 1 Abs. 2 E-VDSG verlangt, dass die Massnahmen über die gesamte Bearbeitungszeit in angemessenen Abständen zu überprüfen sind. Diese Formulierung greift zu kurz. In erster Linie ist die Risikobeurteilung laufend zu überprüfen, woraus sich die Massnahmen und deren Angemessenheit ergeben und somit die allfällige Anpassung von Massnahmen. Zentral ist nämlich, dass einmal getroffene Massnahmen nicht per se weiterbestehen müssen, sondern dass dies ein kontinuierlicher Prozess darstellt, bei dem die Risiken immer wieder von neuem betrachtet, eingeordnet 8nd dagegen entsprechende Mass-nahmen getroffen werden müssen.

4. Zu Art. 2 E-VDSG

Wir regen an, die in dieser Bestimmung beschriebenen Schutzziele, die bereits in Art. 5 Abs. 1 Bst. h rDSG angelegt sind, angepasst an den aktuellen Stand der Technik und in einer verständlichen Weise umzuformulieren. Mögliche diesbezügliche Formulierungen finden sich in § des Informations- und Datenschutzgesetzes des Kantons Basel-Stadt oder § 7 des Informations- und Datenschutzgesetzes des Kantons Zürich.

5. Zu Art. 3 E-VDSG

Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und dann unter Umständen sanktioniert) werden kann.

Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das mittels Protokollierung wirksam reduziert werden kann; dass ein *irgendwie* geartetes Risiko verbleibt, reicht nicht (es fehlt dann an der Verhältnismässigkeit der neuen Datenbearbeitung). Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen offene Berechtigungen implementiert werden müssen, weil nicht zum Vorherein bekannt ist, auf welche konkreten Daten der/die Berechtigte bei der Aufgabenerfüllung Zugang haben muss (z.B. im Schengen-Informationssystem). Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert und

stichprobenweise überprüft werden. Die Pflicht zur Protokollierung ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert.

Für die Bundesorgane soll die Protokollierung für das Bearbeiten *sämtlicher* Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Das geht unseres Erachtens zu weit. Denn festzuhalten ist, dass die Protokollierung selbst eine Beschaffung von Personendaten darstellt, die somit dem Grundsatz der Verhältnismässigkeit genügen muss. Zwar erlaubt Art. 57*l* Bst. b Ziff. 4 RVOG die Aufzeichnung von Randdaten zum Nachvollzug des Zugriffs auf Datensammlungen, aber eben nur insoweit, als die Aufzeichnung verhältnismässig ist. Dass selbst bei einfachen Personendaten und selbst bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht über diese Anforderung hinaus. Es ist nicht klar eruierbar, warum die Pflicht der Bundesorgane zur Protokollierung weitergehen soll als jene der privaten Verantwortlichen. Diese Thematik soll entsprechend nochmals angeschaut werden.

In Art. 3 Abs. 3 E-VDSG sollte vor «die Identität der Empfängerin oder des Empfängers» das Wort «gegebenenfalls» eingefügt werden, da es sich nicht bei jeder protokollierten Bearbeitung um eine Bekanntgabe handelt (sondern teilweise auch «nur» Abfragen getätigt werden, ohne dass Personendaten bekannt gegeben werden).

Gemäss Art. 3 Abs. 4 E-VDSG sind die Protokolle während zwei Jahren aufzubewahren und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei und dafür ist nicht in jedem Fall eine personenbezogene Auswertung erforderlich. Für die Bundesorgane legen die Art. 57*m* ff. RVOG und Art. 8 ff. der zugehörigen Ausführungsverordnung fest, wie die Auswertungen erfolgen dürfen, wobei ggf. auch ein gestaffeltes Vorgehen angezeigt ist (vgl. BGE 143 II 443). Der letzte Satz ist deshalb im Sinne «dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden» zu ergänzen.

6. Zu Art. 4 und 5 E-VDSG

Wir empfehlen, anstelle der zwei in Art. 4 Abs. 1 E-VDSG festgehaltenen alternativen Vorgaben die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 rDSG). Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 rDSG), die Teil des Bearbeitungsreglements sein können.

Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater (DB) ist die Fachperson bei einem Verantwortlichen und ein Bearbeitungsreglement wird zusammen mit ihr erstellt und nicht «der DB in einer für diese verständlichen Form zur Verfügung» gestellt. Es gehört zu den Aufgaben der DB, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b rDSG). Weiter muss die DB über die erforderlichen Fachkenntnisse verfügen (Art. 10 Abs. 3 Bst. c rDSG), was mit der Formulierung, das Bearbeitungsreglement sei ihr «in verständlicher Form» zur Verfügung zu stellen, nicht vereinbar ist, weil letzteres eine Abwertung der Fachkompetenzen impliziert.

Diese Ausführungen gelten analog auch für Art. 5 E-VDSG.

7. Zu Art. 7 E-VDSG

Auch die DB des Bundesorgans hat bei der Anwendung der Datenschutzvorschriften mitzuwirken (vgl. unten Art. 28 E-VDSG). Es widerspricht dem präventiven und risikoorientierten Ansatz des rDSG, wenn die DB lediglich nachträglich über den Abschluss eines Outsourcingvertrags oder bei einer Funktionsübertragung informiert werden soll. Zu den Aufgaben der DB gehört die Involvierung in solche Geschäfte. Die ist eine Kernaufgabe der DB als Beratungsfunktion («Mitwirkung bei der Anwendung der Datenschutzvorschriften»). Die DB ist rechtzeitig zu informieren (und «mit ins Boot zu holen»), wie dies korrekterweise bei Datenbearbeitungsprojekten vorgesehen ist (Art. 31 E-VDSG). Um Kompetenz- und Umsetzungsfragen (vor allem auch der Praxis) bereits im Voraus verhindern zu können, raten wir Ihnen, diese Bestimmung und darin vor allem die Position der DB entsprechend der Definition im rDSG zu stärken.

8. Zu Art. 8 E-VDSG

Bei den Formulierungen in dieser Bestimmung fällt auf, dass der EDÖB (formell) konsultiert wird, und die Beurteilungen von internationalen Organisationen oder ausländischen Behörden berücksichtigt werden können (materiell). Es ist klar zu formulieren, dass auch die Stellungnahmen des EDÖB materiell zu berücksichtigen sind, zumal sich die Erläuterungen hierzu nicht äussern (Erläuterungen, S. 27).

9. Zu Art. 9 Abs. 3 E-VDSG

Gemäss Art. 16 Abs. 2 Bst. b und c rDSG sind Datenschutzklauseln und spezifische Garantien dem EDÖB vorgängig mitzuteilen. Der Einleitungssatz von Art. 9 Abs. 3 E-VDSG suggeriert, dass es einen Sachverhalt geben könnte, in der auch die Nicht-Mitteilung zu einer rechtskonformen Bekanntgabe ins Ausland führen würde. Wir empfehlen, diese Formulierung entsprechend anzupassen.

10. Zu Art. 19 E-VDSG

Art. 24 Abs. 1 rDSG sieht eine Meldung von Verletzungen der Datensicherheit in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 rDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 rDSG).

Art. 24 rDSG ist eine (bewusst) abweichende Bestimmung von Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO aufgenommen. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen. Für die Mehrheit der Verantwortlichen trifft dies aber nicht zu. Art. 19 E-VDSG bringt somit unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht (die in der Praxis zudem möglichst rasch erfolgen soll) wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde rasch informiert wird, allenfalls auch die betroffenen Personen, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden. Es erscheint also fraglich, ob Art. 24 rDSG die in Art. 19 E-VDSG enthaltene Konkretisierung überhaupt braucht.

11. Zu Art. 20 E-VDSG

Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 rDSG definiert. Daraus ergeben sich Umfang und Zweck der Auskunft, was sich nach objektiven Kriterien misst. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte. Wir regen deshalb dazu an, Art. 20 Abs. 3 E-VDSG zu streichen.
Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen». Dies ergibt sich bereits aus Art. 8 rDSG und den Bestimmungen des 1. Kapitels der E-VDSG, weshalb diese Bestimmung gestrichen werden kann und soll.

Art. 26 Abs. 4 rDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person. Deshalb ist Art. 20 Abs. 5 E-VDSG ersatzlos zu streichen.

12. Zu Art. 25 E-VDSG

Art. 25 E-VDSG hält fest, welche Aufgaben die DB wahrnehmen muss. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 rDSG, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die er oder sie wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 rDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist missverständlich und entsprechend anzupassen. Dies könnte eventuell bereits mit dem Einfügen eines Passus wie «insbesondere» an geeigneter Stelle umgesetzt werden.

13. Zu Art. 26 E-VDSG noch anschauen

In Anwendung von Art. 12 Abs. 5 rDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn (1) umfangreich besonders schützenswerte Personendaten bearbeitet werden oder (2) ein Profiling mit hohem Risiko durchgeführt wird. Wie bei Art. 4 Abs. 1 E-VDSG ist zu erwähnen, dass diese Eingrenzung nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es unseres Erachtens angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 rDSG).

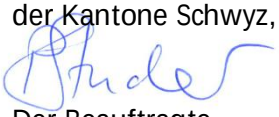
14. Zu Art. 36 E-VDSG

Diese Bestimmung ist überflüssig, weil sich die darin enthaltene Präzisierung bereits aus Art. 39 rDSG ergibt.

Wir hoffen, Ihnen mit diesen Angaben zu dienen, stehen bei Fragen gerne zur Verfügung und danken bereits im Voraus für die Berücksichtigung unserer Hinweise.

Freundliche Grüsse

(Öffentlichkeits- und) Datenschutzbeauftragter
der Kantone Schwyz, Obwalden und Nidwalden



Der Beauftragte
Philipp Studer

Regierung des Kantons St.Gallen

Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Justiz- und
Polizeidepartement
Bundeshaus West
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 74 44
info.sk@sg.ch

St.Gallen, 10. September 2021

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 23. Juni 2021 laden Sie uns zur Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) ein. Wir danken für diese Gelegenheit und nehmen gern wie folgt Stellung:

Da der Geltungsbereich des Datenschutzgesetzes – und damit auch derjenige der VDSG als Ausführungsverordnung des Datenschutzgesetzes – auf private Personen und Bundesorgane beschränkt ist, sind die Kantone vom vorliegenden Revisionsentwurf nicht direkt betroffen. Dennoch ist ein funktionales Datenschutzrecht auf eidgenössischer und europäischer Ebene auch aus Sicht der Kantone von grosser Bedeutung. Dies nicht zuletzt aus wirtschaftlichen Gründen, da etwa in der Schweiz domizilierte, aber international tätige Unternehmen auf praktikable Datenschutzvorschriften angewiesen sind. Mit dem vorliegenden Entwurf der neuen VDSG gelingt die beabsichtigte Harmonisierung mit dem EU- und Schengen-Recht wie auch eine generelle Modernisierung des Datenschutzrechts, was wir sehr begrüssen.

Im Anhang dieses Schreibens haben wir einige Punkte aufgeführt, um deren Prüfung und allenfalls Berücksichtigung wir Sie ersuchen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Im Namen der Regierung

Marc Mächler
Präsident

Dr. Benedikt van Spyk
Staatssekretär

KANTON ST.GALLEN · REGIERUNG ·

Beilage:
Anhang

Zustellung auch per E-Mail (pdf- und Word-Version) an:
jonas.amstutz@bj.admin.ch

Anhang zur Vernehmlassungsantwort «Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)»

Die Regierung des Kantons St.Gallen weist im Zusammenhang mit der genannten Vorlage im Einzelnen auf folgende Punkte hin:

Art. 6
Auftragsverarbeitungsverträge sind ein Kernanliegen in der Konzeption der Datenschutz-Grundverordnung der EU (nachfolgend EU-DSGVO). Der zwingend notwendige Inhalt solcher Verträge ist in Art. 28 Abs. 3 EU-DSGVO geregelt und umfasst den Gegenstand, die Dauer, die Art und den Zweck der Datenbearbeitung, die Art der Personendaten, die Kategorien betroffener Personen sowie die Pflichten und Rechte des Verantwortlichen. Als Orientierungshilfe für Verantwortliche und Auftragsbearbeiter könnte dieser Mindestinhalt in Art. 6 des vorliegenden Entwurfs zur Totalrevision der VDSG (nachfolgend E-VDSG) aufgeführt werden.

Art. 17
Die Bestimmung könnte zum Schutz der betroffenen Person insofern präzisiert werden, als die automatisierte Einzelentscheidung bis zum Prüfbescheid durch die natürliche Person keine Wirkung entfalten darf.

Art. 20 Abs. 1 und 2
Zwar klärt der erläuternde Bericht darüber auf, dass zur schriftlichen Form auch die elektronische Form gehört, allerdings wird dies in Art. 20 E-VDSG nicht erwähnt. Um Unsicherheiten bei der Rechtsanwendung zu vermeiden, wäre eine entsprechende Klarstellung in Art. 20 E-VDSG empfehlenswert.

Art. 21 Abs. 2
Die in dieser Bestimmung vorgesehene Verlagerung der Auskunftspflicht vom Verantwortlichen zum Auftragsbearbeiter erscheint heikel, da dadurch die gesetzliche Zuständigkeitsregelung von Art. 25 Abs. 4 nDSG untergraben wird. Die Auskunftspflicht sollte trotz Beizugs eines Auftragsbearbeiters stets beim Verantwortlichen bleiben. Liegen dem Verantwortlichen die benötigten Informationen nicht vor, muss er sie beim Auftragsbearbeiter beschaffen. Vor diesem Hintergrund regen wir die Streichung von Art. 21 Abs. 2 E-VDSG an.

Art. 23 Abs. 1
Art. 25 Abs. 6 nDSG legt fest, dass bei unverhältnismässigem Aufwand vom Grundsatz der Kostenlosigkeit der Auskunftserteilung abgesehen werden kann. Art. 23 Abs. 1 E-VDSG wiederholt den Begriff des «unverhältnismässigen Aufwands», ohne ihn zu präzisieren. Auch dem entsprechenden Abschnitt im erläuternden Bericht ist nichts Konkretes dazu zu entnehmen. Aus diesem Grund, und weil zudem eine Kostenauferlegung das Recht der betroffenen Person auf Auskunft untergraben könnte, regen wir eine ausreichende Konkretisierung des Begriffs auf Verordnungsstufe an.

Art. 25 Abs. 1 Bst. a und b
Nach Art. 10 Abs. 2 nDSG ist die Datenschutzberaterin oder der Datenschutzberater Anlaufstelle für die betroffenen privaten Personen und für die Behörden. Sie oder er ist na-

mentlich für die Schulung und Beratung (Bst. a) sowie für die Mitwirkung bei der Anwendung der Datenschutzvorschriften (Bst. b) zuständig. Art. 25 Abs. 1 Bst. a und b E-VDSG sehen nun aber vor, dass die Datenschutzberaterin oder der Datenschutzberater zusätzlich für die Überprüfung der Bearbeitung von Personendaten sowie die Überprüfung der Datenschutz-Folgenabschätzung zuständig sein soll. Dies würde faktisch zu einer Verlagerung der Verantwortlichkeit vom Verantwortlichen hin zu der oder dem Datenschutzbeauftragten führen, auch wenn eine solche Verlagerung gemäss dem erläuternden Bericht nicht beabsichtigt ist. Unseres Erachtens sollte im Verordnungstext klarer zum Ausdruck kommen, dass keine Verlagerung der Verantwortlichkeit stattfindet.

Kanton Schaffhausen
Volkswirtschaftsdepartement
Mühlentalstrasse 105
CH-8200 Schaffhausen
www.sh.ch

T +41 52 632 73 80
sekretariat.vd@sh.ch

Volkswirtschaftsdepartement

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-
Suter

per E-Mail an:
jonas.amstutz@bj.admin.ch

Schaffhausen, 13. Oktober 2021

Vernehmlassung EJPD betreffend Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Juni 2021 haben Sie uns den Entwurf in obgenannter Angelegenheit zur Stellungnahme unterbreitet. Wir bedanken uns für diese Gelegenheit und nehmen wie folgt Stellung:

Das revidierte Bundesgesetz über den Datenschutz vom 25. September 2020 (nDSG) beinhaltet zahlreiche Delegationsnormen, auf die sich der vorgelegte Verordnungsentwurf (E-VDSG) stützt (siehe Ingress E-VDSG). Zudem konkretisiert der E-VDSG verschiedene Bestimmungen des nDSG.

Der Vernehmlassungsentwurf übernimmt dabei zum Teil überholte Begriffe und Bestimmungen der bisherigen Verordnung und die neuen Ausführungsbestimmungen weisen nicht die notwendige Detaillierung für die Umsetzung des sehr komplexen nDSG auf. Wir bezweifeln deshalb, dass die Verordnung in der jetzigen Ausgestaltung den Verantwortlichen – private Personen wie auch Bundesorgane –die notwendige Hilfe bei der Umsetzung der gesetzlichen Vorgaben bietet.

Bedarf sehen wir insbesondere in den im Folgenden erwähnten Punkten:

Art. 1 bis 4 E-VDSG (Datensicherheit)

In Art. 1 bis 4 E-VDSG werden die Anforderungen an die Datensicherheit (Art. 8 nDSG) konkretisiert. Dabei verlangt Art. 8 Abs. 3 nDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt.

Der E-VDSG konkretisiert diese Mindestanforderungen nicht in einer Form, die auch in Bezug auf die strafrechtlich sanktionierte Unterlassung der Umsetzung der Mindestanforderungen (Art. 61 Abs. 1 lit. c nDSG) objektive Tatbestandsmerkmale erkennen lassen würde.

In Bezug auf die Datensicherheit ist im IT-Recht heute ein Standard erreicht, der klar nach zunächst erfolgender Beurteilung des Schutzbedarfs und der Risiken die entsprechenden Sicherheitsmassnahmen vorschlägt und einteilt (Grundschutz, hoher Schutz, sehr hoher Schutz). Der Bund hat kürzlich mit der Verabschiedung des Bundesgesetzes über die Informationssicherheit (Informationssicherheitsgesetz, [ISG] vom 18. Dezember 2020) gezeigt, wie die heutigen Anforderungen auch gesetzestechnisch umgesetzt werden können. Im E-VDSG wird dagegen am Konzept der bisherigen Verordnung festgehalten. Art. 8 nDSG wird damit nicht praxistauglich konkretisiert.

Der Abschnitt 1 (Datensicherheit) ist deshalb konzeptionell in Anlehnung an das ISG anzupassen.

Art. 1 E-VDSG (Grundsätze)

Es ist klarer zu umschreiben, dass eine zweistufige Vorgehensweise Platz greifen muss, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

Zunächst sind die Schutzziele, der Schutzbedarf und die Risiken zu beurteilen. Die Schutzziele sind bereits in Art. 5 Abs. 1 lit. h nDSG angelegt (vgl. S. 15 der Erläuterungen) und werden in Art. 2 E-VDSG ausführlich aufgezählt. Der Schutzbedarf ergibt sich aus der Art der Daten (Personendaten, besonders schützenswerte Personendaten) und der Datenbearbeitung selbst (z.B. Profiling).

Erst dann erfolgt die Risikobeurteilung, wie dies auch die Datenschutz-Folgenabschätzung vorsieht (Art. 22 nDSG). Die Kriterien «Zweck, Art, Umfang und Umstände der Datenbearbeitung» beziehen sich somit auf die Schutzbedarfsfeststellung (welche bereits eine

erste grobe Einschätzung des möglichen Schadensausmasses enthält). Die Kriterien «Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen» beziehen sich auf die Risikobeurteilung.

Wenn es um die Beurteilung der Angemessenheit der Massnahmen geht, sind die Kriterien «Stand der Technik und Implementierungskosten» einschlägig. Sie sagen aber nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche Massnahme dem Risiko mit der nötigen Effektivität begegnet. Dies ist im erwähnten ISG so angelegt, aber auch in Art. 32 DSGVO, welche Bestimmung in den Erläuterungen (Art. 15) in diesem Zusammenhang explizit erwähnt wird.

Art. 1 Abs. 1 E-VDSG ist im Hinblick auf diese abgestufte Vorgehensweise zu überarbeiten.

Art. 2 E-VDSG (Schutzziele)

Die Schutzziele sollten wie im ISG zusammengefasst werden in Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit. Der Einleitungssatz ist missverständlich: Schutzziele sind Zielvorgaben. Die Massnahmen müssen sich an den in der Risikobeurteilung festgestellten Risiken und nicht an den Schutzzielen orientieren.

Art. 3 E-VDSG (Protokollierung)

Die für Bundesorgane vorgesehene umfassende Protokollierung der Datenbearbeitungen geht zu weit. Eine Protokollierung stellt ihrerseits eine (zusätzliche) Datenbearbeitung dar, die verhältnismässig sein muss. Sie muss ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das durch die Protokollierung wirksam reduziert werden kann.

Geboten scheint eine Protokollierung der Datenbearbeitungen vor allem dort, wo aus betrieblichen Gründen zu umfassende Berechtigungen vergeben werden müssen, weil nicht zum Vornherein bekannt ist, auf welche konkreten Daten die Berechtigten bei der Aufgabenerfüllung Zugang haben müssen (z.B. die Polizeiorgane im Schengen-Informationssystem).

Es erscheint zweckmässig, die Bundesorgane in Absatz 1 aufzunehmen und auf Absatz 2 zu verzichten.

Bei der Auswertung von Datenbearbeitungsprotokollen kann der Verhältnismässigkeit unter Umständen durch ein gestaffeltes Vorgehen Rechnung getragen werden (vgl. BGE 143 II 443). Dies könnte in Abs. 3 zum Ausdruck gebracht werden mit der Formulierung «dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden».

Art. 4 E-VDSG (Bearbeitungsreglement von privaten Personen)

Die in Abs. 1 definierten Voraussetzungen für eine Pflicht zur Erstellung eines Bearbeitungsreglements sind zu eng. Sachgerechter wäre es, die Voraussetzungen für die Datenschutz-Folgenabschätzung gemäss Art. 22 Abs. 1 nDSG zu übernehmen: «Die Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen».

Abs. 3 verkennt die Funktion und Bedeutung des internen Datenschutzberaters bzw. der internen Datenschutzberaterin. Er/sie dürfte es gerade sein, der/die als Fachperson die Erarbeitung eines Bearbeitungsreglements wesentlich mitprägt. Die Formulierung, es sei ihm oder ihr ein Bearbeitungsreglement «in verständlicher Form zur Verfügung zu stellen» verkennt seine/ihre Funktion und Fachkompetenz. Abs. 3 sollte ersatzlos gestrichen werden.

Art. 5 E-VDSG (Bearbeitungsreglement von Bundesorganen)

Vgl. die Vorbehalte bezüglich Art. 4.

Art. 7 E-VDSG (Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans)

Wir erachten es als wenig zielführend, den Datenschutzberater bzw. die Datenschutzberaterin erst nach Abschluss eines Outsourcing-Vertrages zu orientieren. Letztere haben vielmehr bei der Anwendung sämtlicher Datenschutzvorschriften miteinbezogen zu werden (vgl. Art. 28 und Art. 31 E-VDSG).

Art. 7 kann ersatzlos gestrichen werden.

Art. 8 E-VDSG (Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs)

Aus den Erläuterungen (S. 27) scheint hervorzugehen, dass der EDÖB nur formell konsultiert werden soll, während die Beurteilungen von internationalen Organisationen oder ausländischen Behörden materiell berücksichtigt werden können. Es ist in diesem Zusammenhang klarer zum Ausdruck zu bringen, dass auch die Stellungnahmen des EDÖB materiell zu berücksichtigen sind.

Art. 9 E-VDSG (Datenschutzklauseln und spezifische Garantien)

Gemäss Art. 16 Abs. 2 lit. b und c nDSG sind Datenschutzklauseln und spezifische Garantien dem EDÖB vorgängig mitzuteilen. Dies darf in Art. 9 Abs. 3 E-VDSG nicht abgeschwächt werden.

Art. 19 E-VDSG (Meldung von Verletzungen der Datensicherheit)

Art. 24 Abs. 1 nDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 nDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 nDSG).

Der Gesetzgeber weicht in Art. 24 nDSG bewusst ab von der strengeren europäischen Regelung in Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO übernommen. Dies ist einzig für Private dienlich, die auch der DSGVO unterliegen, etwa weil sie Ihre Produkte bzw. Dienstleistungen auch im EU-Raum anbieten. Für eine Vielzahl Privater ist dies nicht der Fall, und Art. 19 E-VDSG bringt unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde und allenfalls auch die betroffenen Personen rasch informiert werden, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden.

Art. 24 nDSG braucht die in Art. 19 E-VDSG enthaltene Konkretisierung nicht. Sie ist wegzulassen.

Art. 20 E-VDSG (Modalitäten des Auskunftsrechts)

Art. 25 nDSG und Art. 26 nDSG regeln das Auskunftsrecht und dessen Einschränkungen ausführlich. Art. 20 E-VDSG bringt hierzu einige Konkretisierungen, die über das Notwendige hinausgehen.

Gemäss Art. 20 Abs. 3 E-VDSG muss die Auskunft für die betroffene Person verständlich sein. Umfang und Zweck der Auskunft ist in Art. 25 Abs. 2 nDSG definiert. Es muss ein objektiver Massstab angelegt werden; das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte. Dies ist aus datenschutzrechtlicher Sicht kontraproduktiv.

Art. 20 Abs. 3 E-VDSG ist ersatzlos zu streichen.

Die in Art. 20 Abs. 4 E-VDSG stipulierte Auflage an die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen» ist unnötig, da sie sich bereits aus Art. 8 nDSG und den Bestimmungen des 1. Kapitels der E-VDSG ergibt. Sie ist in Art. 20 Abs. 4 E-VDSG zu streichen.

Art. 26 Abs. 4 nDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand ohne Mehrwert für die betroffene Person.

Art. 20 Abs. 5 E-VDSG ist ersatzlos zu streichen.

Art. 21 E-VDSG (Zuständigkeit)

Art. 21 Abs. 1 E-VDSG sieht vor, dass ein Verantwortlicher, der für die Behandlung des Begehrens nicht zuständig ist, dieses an den zuständigen Verantwortlichen weiterleitet. Dieser verwaltungsrechtliche Grundsatz gilt für die Bundesorgane auch ohne Erwähnung in diesem Zusammenhang. Die gleiche Auflage auch dem privatrechtlichen Verantwortlichen zu machen, erscheint unverhältnismässig. Sie führt zu einem unter Umständen grossen Aufwand für den privatrechtlichen Verantwortlichen, den «zuständigen» Verantwortlichen ausfindig zu machen, ohne dass dadurch die Rechte der betroffenen Personen gestärkt würden.

Art. 21 Abs. 1, 2. Satz E-VDSG ist daher ersatzlos zu streichen.

Art. 24 E-VDSG (Datenportabilität)

Der pauschale Verweis auf die Anwendung von Bestimmungen zum Auskunftsrecht zur Konkretisierung von Art. 28 nDSG greift zu kurz. Er wird dem neuen Rechtsinstitut der «Datenportabilität» nicht gerecht und verkennt den durchaus vorhandenen Bedarf einer Konkretisierung der gesetzlichen Bestimmung (beispielsweise in Bezug auf die «gängigen elektronischen Formate» oder den «unverhältnismässigen Aufwand» bei der direkten Übertragung von einem Verantwortlichen zu einem anderen). Zudem wäre auch in Bezug auf die Ausnahmen der Kostenlosigkeit eine andere Regelung als beim Auskunftsrecht denkbar, da hier nicht der Persönlichkeitsschutz, sondern der wirtschaftliche Wert der Daten im Vordergrund steht.

Es sind in Art. 24 E-VDSG eigene Regelungen vorzusehen.

Art. 25 E-VDSG (Datenschutzberaterin oder Datenschutzberater)

Die gesetzlichen Aufgaben der Datenschutzberaterin oder des Datenschutzberaters sind gemäss Art. 10 Abs. 2 nDSG umfassend. Es muss in Art. 25 E-VDSG klarer zum Ausdruck gebracht werden, dass nicht auf Verordnungsstufe eine Einschränkung des Aufgabenbereichs vorgenommen werden soll, sondern dass es sich um eine lediglich teilweise Konkretisierung handelt.

Art. 26 E-VDSG (Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten)

Wie oben bei Art. 4 Abs. 1 E-VDSG ist darauf hinzuweisen, dass die eingrenzende Aufzählung in Art. 26 E-VDSG bei Weitem nicht alle für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 nDSG).

Art. 28 E-VDSG (Anforderungen und Aufgaben)

In der Aufzählung von Art. 28 Abs. 2 E-VDSG muss auch die in Art. 10 Abs. 2 lit. b nDSG festgelegte Aufgabe – die Mitwirkung bei der Anwendung der Datenschutzvorschriften – erwähnt werden, und nicht nur die Schulung und Beratung (Art. 10 Abs. 2 lit. a nDSG).

Art. 36 E-VDSG (Datenbearbeitung zu nicht personenbezogenen Zwecken)

Diese Bestimmung kann gestrichen werden, da sich die Präzisierung bereits klar aus Art. 39 nDSG ergibt.

Für die Kenntnisnahme und Berücksichtigung unserer Stellungnahme danken wir Ihnen.

Freundliche Grüsse

Volkswirtschaftsdepartement
Der Vorsteher:

Dino Tamagni
Regierungsrat

KANTON solothurn

Regierungsrat

Rathaus / Barfüssergasse
4509 Solothurn
so.ch

Bundesamt für Justiz
Bundesrain 20
3003 Bern

28. September 2021

Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Die Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements hat uns mit Schreiben vom 23. Juni 2021 eingeladen, zum Vernehmlassungsentwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11) und zu den Ausführungen im erläuternden Bericht Stellung zu nehmen. Wir nehmen hiermit zu den genannten Unterlagen Stellung, soweit der Kanton Solothurn durch die Änderungen direkt oder indirekt betroffen ist. Die Aussagen sind in der beiliegenden Tabelle aufgeführt.

Wir danken Ihnen, dass wir zur Vorlage Stellung nehmen können. Wir senden die Unterlagen in elektronischer Form an jonas.amstutz@bj.admin.ch.

Mit freundlichen Grüssen

IM NAMEN DES REGIERUNGSRATES

sig.
Susanne Schaffner
Frau Landammann

sig.
Andreas Eng
Staatsschreiber

Beilage: Tabelle Stellungnahme

IIIIII KANTON solothurn

Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz
Tabelle Stellungnahme

Entwurf VDSG	Bemerkungen/Anregungen
Art. 3 Protokollierung [1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. [2] Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. (…)	Bemerkung: Die umfassende Protokollierungspflicht für Bundesorgane geht zu weit und ist nicht angemessen. Es können in diesem Punkt für Bundesorgane die gleichen Anforderungen wie für private Verantwortliche angewendet werden. Änderungsvorschlag: [1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der ~~private~~ Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. ~~[2] Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.~~
Art. 4 Bearbeitungsreglement von privaten Personen [1] Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie: a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen. (…) [3] Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.	Bemerkung zu Abs. 1: Zunächst ist die Eingrenzung der Pflicht zur Erstellung eines Reglements auf die Fälle nach Abs. 1 Bst. a und b zu eng. Die Revision des DSG ist gekennzeichnet durch einen risikobasierten Ansatz. In zahlreichen Bestimmungen werden Rechtswirkungen an das Vorliegen eines «hohen Risikos für die Persönlichkeit oder die Grundrechte der betroffenen Person» angeknüpft. Es ist nicht ersichtlich, weshalb von diesem Massstab – der u.a. für die Erstellung einer Datenschutz-Folgenabschätzung gilt (vgl. Art. 22 Abs. 1 nDSG) – vorliegend abgewichen wird. Ein hohes Risiko kann etwa bei der Bearbeitung von umfangreichen gewöhnlichen Personendaten bestehen. Immerhin können die Buchstaben a und b als nicht abschliessende Beispiele, für Fälle in denen stets ein hohes Risiko vorliegt, beibehalten werden. Änderungsvorschlag zu Abs. 1: [1] Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn **die Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich**

	bringen kann. Ein hohes Risiko liegt namentlich vor, wenn: a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen. Bemerkung zu Abs. 3: Ferner ist unklar was mit dem Zusatz in Absatz 3, wonach das Reglement in einer für die Datenschutzberaterin oder den Datenschutzberater «verständlichen Form» zur Verfügung gestellt werden muss, gemeint ist. Unverständlich darf das Bearbeitungsreglement nie sein. Das versteht sich von selbst. Dass das Reglement allenfalls für Laien unverständlich sein kann, ist unbeachtlich, handelt es sich bei der Datenschutzberaterin oder dem Datenschutzberater doch um eine qualifizierte Fachperson (vgl. Art. 10 Abs. 3 Bst. c nDSG sowie Art. 28 Abs. 1 Bst. a E-VDSG). Schliesslich sollte zumindest in den Erläuterungen klargestellt werden, dass die Bestellung einer Datenschutzberaterin oder eines Datenschutzberaters gemäss Art. 10 nDSG freiwillig erfolgt. Änderungsvorschlag zu Abs. 3: 3 Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater ~~in einer für diese oder diesen verständlichen Form~~ zur Verfügung stellen.
Art. 5 Bearbeitungsreglement von Bundesorganen (…) 3 Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen.	Bemerkung: Es kann auf die Bemerkung zu Art. 4 E-VDSG verwiesen werden. Änderungsvorschlag: 3 Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater ~~in einer für diese oder diesen verständlichen Form~~ sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen
Art. 7 Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten.	Bemerkung: Art. 7 ist überflüssig und irreführend. Gemäss Art. 10 Abs. 2 Bst. b nDSG wirkt der Datenschutzberater ohnehin bei der Anwendung der Datenschutzvorschriften mit. Dieser Anforderung trägt Art. 7 zu wenig Rechnung, indem der Berater erst *nach* Abschluss eines Auftragsbearbeitungsvertrages informiert wird. Im Übrigen

Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften entstehen.	bringt die Bestimmung keinen Mehrwert und kann demnach ersatzlos gestrichen werden. Änderungsvorschlag: ~~Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften.~~
Art. 12 Verhaltenskodizes und Zertifizierungen (…) 3 Der Verhaltenskodex oder die Zertifizierung muss mit einer verbindlichen und durchsetzbaren Verpflichtung des Verantwortlichen oder des Auftragsbearbeiters im Drittstaat verbunden werden, die darin enthaltenen Massnahmen anzuwenden.	Bemerkung: Der Charakter der «durchsetzbaren Verpflichtung» ist zu präzisieren. In gewissen Staaten werden rechtliche Verpflichtungen rein theoretisch zwar durchsetzbar sein, praktisch gesehen dürften die realistischen Durchsetzungsmöglichkeiten aber gering bleiben, sei dies aufgrund von rechtlichen Hürden, überlasteter Verwaltung und Justiz, Korruption oder dergleichen. Wichtig ist, dass die Durchsetzbarkeit der Verpflichtung ohne unverhältnismässigen Aufwand möglich ist. Im Übrigen sollte aus den Erläuterungen klar hervorgehen, dass Verhaltenskodizes nur von Verbänden und nicht von einzelnen Verantwortlichen stammen können (vgl. Botschaft nDSG, 7035). Änderungsvorschlag: 3 Der Verhaltenskodex oder die Zertifizierung muss mit einer verbindlichen und **mit verhältnismässigen Aufwand** durchsetzbaren Verpflichtung des Verantwortlichen oder des Auftragsbearbeiters im Drittstaat verbunden werden, die darin enthaltenen Massnahmen anzuwenden.
Art. 13 Modalitäten der Informationspflicht 1 Der Verantwortliche und der Auftragsbearbeiter teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit. 2 Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.	Bemerkung: Zu begrüssen ist, dass darauf verzichtet wird die Information durch einen sogenannten Medienbruch allgemein zu legitimieren. Ein Medienbruch liegt beispielsweise dann vor, wenn in einem abgedruckten Vertrag auf einen QR-Code oder bei einem Telefonat auf einen URL-Link verwiesen wird, worüber die betroffene Person an die zu erteilenden Informationen gelangen kann. Ob der Informationspflicht durch derartige Informationsmethoden genüge getan ist, muss anhand von Art. 19 Abs. 1 nDSG beurteilt werden, wonach die Information «angemessen» zu sein hat. Es gelten dabei der Verhältnismässigkeitsgrundsatz und der risikobasierte Ansatz. Es sind die aus der Datenbearbeitung

	resultierenden Risiken für die betroffene Person und der Aufwand des Verantwortlichen für die Informationserbringung gegeneinander abzuwägen. Bei einer Bearbeitung von besonders schützenswerten Personendaten wird die Information über einen Medienbruch regelmässig unangemessen sein und somit den gesetzlichen Anforderungen nicht genügen. Eine allgemeine und pauschale Legitimierung des Medienbruchs – wie teilweise gefordert – ist abzulehnen.
Art. 20 Modalitäten [1] Das Auskunftsbegehren wird schriftlich gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden. (…)	Bemerkung: Art. 25 nDSG schreibt die Schriftlichkeit eines Auskunftsbegehrens nicht mehr vor. Der erste Satz von Art. 20 Abs. 1 E-VDSG verlangt eine solche jedoch in absoluter Form. Diese wird zwar durch Satz 2 relativiert. Die Bestimmung ist dadurch aber widersprüchlich, und der erste Satz verletzt in dieser Form Art. 25 nDSG. Ein Auskunftsbegehren soll generell in schriftlicher und in mündlicher Form möglich sein. Dies hat gleichzeitig zur Folge, dass das Gesuch auch denjenigen Personen offensteht, für welche die Schriftlichkeit eine schwer oder nicht überwindbare Hürde darstellen würde. Änderungsvorschlag: [1] Das Auskunftsbegehren ~~wird~~ **kann** schriftlich **oder mündlich** gestellt **werden**. ~~Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden~~
Art. 21 Zuständigkeit [1] Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter. (…)	Bemerkung: Der zweite Satz von Abs. 1 bewirkt für private Verantwortliche einen unverhältnismässigen Aufwand. Für Bundesorgane ergibt sich dieser Grundsatz hingegen ohnehin aus dem Verwaltungsrecht. Insofern kann der zweite Satz ersatzlos gestrichen werden. Änderungsvorschlag: [1] Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. ~~Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.~~
Art. 22 Frist [1] Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt,	Bemerkung: Damit eindeutig klar ist, dass die Auskunft *in der Regel* innert 30 Tagen erteilt wird, wie es Art. 25 Abs. 7 nDSG verlangt, sollte dies auch aus der

muss er dies innert derselben Frist mitteilen. [2] Kann die Auskunft nicht innert 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber benachrichtigen und ihr die Frist mitteilen, in der die Auskunft erfolgen wird.	Verordnungsbestimmung explizit hervorgehen. Änderungsvorschlag: [1] Die Auskunft wird **in der Regel** innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen. Bemerkung: Aus dem Wortlaut von Absatz 2 muss klar hervorgehen, dass die Überschreitung der 30-tägigen Frist die *Ausnahme* bleibt. Ausserdem ist sicherzustellen, dass die verlängerte Frist *angemessen* bleibt und nicht nach Belieben des Verantwortlichen ausfallen kann. Änderungsvorschlag: [2] Kann die Auskunft **ausnahmsweise** nicht innert 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber benachrichtigen und ihr ~~die~~ **eine angemessene** Frist mitteilen, in der die Auskunft erfolgen wird.
Art. 23 Ausnahmen von der Kostenlosigkeit (…) [2] Die Beteiligung beträgt maximal 300 Franken. (…)	Bemerkung: Es ist zu begrüssen, dass der Kostenbeteiligung in Absatz 2 klare und für die betroffenen Personen verhältnismässige Grenzen gesetzt werden. Weil Auskunftsgesuche in Ausnahmefällen aber einen beträchtlichen Aufwand für Verantwortliche generieren können, ist fraglich, ob eine Obergrenze von maximal CHF 500 zu bevorzugen wäre. Abzulehnen weil unzumutbar sind indessen sicherlich Kostenbeteiligungen im vierstelligen Bereich. Änderungsvorschlag: [2] Die Beteiligung beträgt maximal **500** Franken.
Art. 26 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt.	Bemerkung: Die Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten für die Konstellationen nach Bst. a und b zu weit. Es ist nicht ersichtlich, weshalb vom Massstab zur Erstellung einer Datenschutz-Folgenabschätzung, wie in Art. 22 Abs. 1 nDSG vorgesehen, abgewichen wird. Dieser risikobasierte Massstab (*hohes Risiko* für die Persönlichkeit oder die Grundrechte der betroffenen Person) durchzieht das nDSG und ist auch hier zu übernehmen. Immerhin können die Buchstaben a und b als nicht abschliessende

a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.	Beispiele für, wann ein hohes Risiko vorliegt, beibehalten werden. Änderungsvorschlag: Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, **sofern ihre Bearbeitungstätigkeiten kein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen. Ein hohes Risiko liegt namentlich vor, wenn:** ~~ausser eine der folgenden Voraussetzungen ist erfüllt.~~ a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.
Verordnung über das Strafregister vom 29. September 2006 (VOSTRA-Verordnung; SR 331) Art. 18 Sorgfaltspflichten und Datenbearbeitungsgrundsätze (…) 5 Die Strafregisterdaten nach Artikel 366 Absätze 2 bis 4 StGB dürfen nicht isoliert in einer neuen Datenbank gespeichert oder aufbewahrt werden, es sei denn, dies sei zur Begründung eines getroffenen Entscheides, einer erlassenen Verfügung oder eines eingeleiteten Verfahrensschritts notwendig. (…)	Bemerkung: Mit Inkrafttreten des Strafregistergesetzes, voraussichtlich 2023, wird den kantonalen Polizeistellen Zugriff auf das Strafregister gewährt, u.a. für die Erkennung oder Verhütung von Straftaten (Art. 38 i.V.m. Art. 46). Für die Polizei werden u.a. Grundurteile ersichtlich, die ein Tätigkeitsverbot oder ein Kontakt- und Rayonverbot nach Art. 67 ff. StGB enthalten. Die Kenntnis eines solchen Verbots ist primär zur Verbotsdurchsetzung von Bedeutung, konkret zur Gewährleistung, dass der Verbotszweck (Verhinderung einer weiteren, schweren Straftat) tatsächlich erreicht wird. Das zentrale Informationssystem der Polizei enthält u.a. Hinweise über geltende Wegweisungen und Rückkehrverbote nach ZGB und nach kantonalem Recht. Zur Gefahrenabwehr und Straftatenverhütung stehen die Daten insb. den intervenierenden Polizeiangehörigen vor Ort zur Verfügung. Dasselbe sollte auch für die Verbote nach Art. 67 ff. StGB möglich sein, dürfte von engen Wortlaut im Entwurf allerdings nicht gedeckt sein. Änderungsvorschlag: 5 Die Strafregisterdaten nach Artikel 366 Absätze 2 bis 4 StGB dürfen nicht isoliert in einer neuen Datenbank gespeichert oder aufbewahrt werden, es sei denn, dies sei zur Begründung **oder Durchsetzung** eines getroffenen Entscheides, einer erlassenen Verfügung oder eines eingeleiteten Verfahrensschritts notwendig.

Regierungsrat des Kantons Schwyz

VERSENDET AM 05. OKT. 2021

kantonschwyz

6431 Schwyz, Postfach 1260

per E-Mail
Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

jonas.amstutz@bj.admin.ch

Schwyz, 28. September 2021

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
Vernehmlassung des Kantons Schwyz

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 23. Juni 2021 haben Sie die Kantonsregierungen eingeladen, zur oben erwähnten Vernehmlassungsvorlage bis 14. Oktober 2021 Stellung zu nehmen. Für diese Einladung danken wir Ihnen bestens und nehmen zu nachfolgenden Bestimmungen gerne wie folgt Stellung:

Allgemeines
Der Vernehmlassungsentwurf erfüllt die Erwartungen an eine klare, verständliche, stufengerechte und anwenderfreundliche Vollzugsordnung nur bedingt. Einerseits enthält der Verordnungsentwurf Vorschriften, die auf Gesetzesstufe hätten verankert werden müssen (Umfang der Protokollierungspflicht, Differenzierungen beim Profiling, Informationspflichten), andererseits werden auf Verordnungsstufe allgemeine Vorgaben gemacht, wo den datenschutzverantwortlichen Organen Raum für spezifische Umsetzungslösungen in Form von Datenschutzreglementen, Weisungen und Anleitungen belassen werden müsste (z. B. Vorgaben zu den Protokollauswertungen, Aufbewahrung von Datenschutzfolgeabschätzungen). Letztlich geht es darum, dass die datenschutzrechtlichen Vorgaben im Sinne einer Querschnittsfunktion in die einzelnen öffentlichen Aufgaben implementiert werden können und nicht umgekehrt, dass sich die staatliche Aufgabenerfüllung dem Datenschutzregime unterzuordnen hat.

Art. 1 – 4 E-VDSG (Datensicherheit)
Die Art. 1 bis 4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 rDSG). Dabei verlangt Art. 8 Abs. 3 rDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt. Der E-VDSG hält am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht, ohne aber Art. 8 rDSG für die Praxis zu konkretisieren. Eine solche Konkretisierung wäre aber gerade für die verantwortlichen öffentlichen Organe (also Bundesorgane) und Private sehr wichtig und entscheidend. Denn sie müssen erkennen

können, was sie im Bereich der Datensicherheit tun müssen und wie dies erfolgen könnte (z. B. anhand von Leitlinien)

Art. 1 E-VDSG (Grundsätze)
Aus Art. 1 Abs. 1 E-VDSG ergibt sich, dass die Angemessenheit von Massnahmen sich nach den Kriterien Zweck, Art, Umfang und Umstände der Datenbearbeitung, Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen, Stand der Technik und Implementierungskosten beurteilt. Dabei sagen die für die Beurteilung der Angemessenheit der Massnahmen bestehenden Kriterien «Stand der Technik und Implementierungskosten» wohl nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche dem Risiko mit der nötigen Effektivität begegnet. Dies wird beispielsweise auch in Art. 32 DSGVO so geregelt.

Art. 1 Abs. 2 E-VDSG verlangt, dass die Massnahmen über die gesamte Bearbeitungszeit in angemessenen Abständen zu überprüfen sind. Diese Formulierung greift zu kurz. In erster Linie ist die Risikobeurteilung laufend zu überprüfen, woraus sich die Massnahmen und deren Angemessenheit ergeben und somit die allfällige Anpassung von Massnahmen. Zentral ist nämlich, dass einmal getroffene Massnahmen nicht per se weiterbestehen müssen, sondern dass dies ein kontinuierlicher Prozess darstellt, bei dem die Risiken immer wieder von neuem betrachtet, eingeordnet und dagegen entsprechende Massnahmen getroffen werden müssen.

Unklar ist ferner, ob die Angemessenheitskriterien gemäss Art. 1 Abs. 1 kumulativ zu verstehen sind? Dies wie auch die in «angemessenen Abständen», aber in umfassender Weise zu überprüfenden Massnahmen erachten wir nicht als sachgerecht und wirksam.

Art. 2 E-VDSG (Schutzziele)
Wir regen an, die in dieser Bestimmung beschriebenen Schutzziele, die bereits in Art. 5 Abs. 1 Bst. h rDSG angelegt sind, angepasst an den aktuellen Stand der Technik und in einer verständlichen Weise umzuformulieren. Mögliche diesbezügliche Formulierungen finden sich im Informations- und Datenschutzgesetzes des Kantons Basel-Stadt oder im Informations- und Datenschutzgesetzes des Kantons Zürich (§ 7).

Art. 3 E-VDSG (Protokollierung)
Die Protokollierungspflicht soll auf automatisierte Datenbearbeitungsvorgänge, die ein hohes Risiko der Verletzung von Persönlichkeits- bzw. Grundrechten bergen, beschränkt werden. Die hohen Anforderungen an die Zweckbindung und Aufbewahrung der Protokolle erachten wir als nicht zielführend und praxisfremd.
Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und dann unter Umständen sanktioniert) werden kann. Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das mittels Protokollierung wirksam reduziert werden kann; dass ein irgendwie geartetes Risiko verbleibt, reicht nicht (es fehlt dann an der Verhältnismässigkeit der neuen Datenbearbeitung). Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen offene Berechtigungen implementiert werden müssen, weil nicht zum Vorherein bekannt ist, auf welche konkreten Daten der/die Berechtigte bei der Aufgabenerfüllung Zugang haben muss (z. B. im Schengen-Informationssystem). Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert und stichprobenweise überprüft werden. Die Pflicht zur Protokollierung ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert. Für die Bundesorgane soll

die Protokollierung für das Bearbeiten sämtlicher Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Das geht unseres Erachtens zu weit. Denn festzuhalten ist, dass die Protokollierung selbst eine Beschaffung von Personendaten darstellt, die somit dem Grundsatz der Verhältnismässigkeit genügen muss. Zwar erlaubt Art. 57l Bst. b Ziff. 4 RVOG die Aufzeichnung von Randdaten zum Nachvollzug des Zugriffs auf Datensammlungen, aber eben nur insoweit, als die Aufzeichnung verhältnismässig ist. Dass selbst bei einfachen Personendaten und selbst bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht über diese Anforderung hinaus. Es ist nicht klar eruierbar, warum die Pflicht der Bundesorgane zur Protokollierung weitergehen soll als jene der privaten Verantwortlichen. Diese Thematik soll entsprechend nochmals angeschaut werden.
In Art. 3 Abs. 3 E-VDSG sollte vor «die Identität der Empfängerin oder des Empfängers» das Wort «gegebenenfalls» eingefügt werden, da es sich nicht bei jeder protokollierten Bearbeitung um eine Bekanntgabe handelt (sondern teilweise auch «nur» Abfragen getätigt werden, ohne dass Personendaten bekannt gegeben werden).
Gemäss Art. 3 Abs. 4 E-VDSG sind die Protokolle während zwei Jahren aufzubewahren und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei und dafür ist nicht in jedem Fall eine personenbezogene Auswertung erforderlich. Für die Bundesorgane legen die Art. 57m ff. RVOG und Art. 8 ff. der zugehörigen Ausführungsverordnung fest, wie die Auswertungen erfolgen dürfen, wobei ggf. auch ein gestaffeltes Vorgehen angezeigt ist (vgl. BGE 143 II 443). Der letzte Satz ist deshalb im Sinne «dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden» zu ergänzen.

Art. 4 und 5 E-VDSG (Bearbeitungsreglement von privaten Personen / Bundesorganen)
Wir empfehlen, anstelle der zwei in Art. 4 Abs. 1 E-VDSG festgehaltenen alternativen Vorgaben die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 rDSG). Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 rDSG), die Teil des Bearbeitungsreglements sein können.
Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater (DB) ist die Fachperson bei einem Verantwortlichen und ein Bearbeitungsreglement wird zusammen mit ihr erstellt und nicht «der DB in einer für diese verständlichen Form zur Verfügung» gestellt. Es gehört zu den Aufgaben der DB, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b rDSG). Weiter muss die DB über die erforderlichen Fachkenntnisse verfügen (Art. 10 Abs. 3 Bst. c rDSG), was mit der Formulierung, das Bearbeitungsreglement sei ihr «in verständlicher Form» zur Verfügung zu stellen, nicht vereinbar ist, weil letzteres eine Abwertung der Fachkompetenzen impliziert. Diese Ausführungen gelten analog auch für Art. 5 E-VDSG.

Art. 6 E-VDSG (Bearbeitung durch Auftragsbearbeiter – Modalitäten)
Das verantwortliche öffentliche Organ, welches Daten durch Dritte bearbeiten lässt (sog. Auftragsdatenbearbeitung) bleibt zwar für den Datenschutz verantwortlich, was bereits auf Gesetzesstufe verbrieft ist, jedoch geht daraus nicht hervor, dass es auch sicherstellen muss, dass der Auftragsbearbeiter die Daten auch tatsächlich vertrags- oder gesetzesgemäss bearbeitet. Dies würde auf eine Dauerüberwachung hinauslaufen, was gerade nicht Sinn und Zweck der Auslagerung von Verwaltungstätigkeiten ist. Der Auftragsdatenbearbeitet steht klarerweise in der Mitverantwortung für die auftrags- und rechtskonforme Datenbearbeitung.

Art. 7 E-VDSG (Information an den Datenschutzberater des Bundesorgans)
Die Informationspflicht des verantwortlichen öffentlichen Organs an den Datenschutzberater schiesst über das Ziel hinaus. Der Datenschutzberater ist kein Aufsichtsorgan sondern eine interne Fachperson, welche proaktiv und situativ in geplante Datenbearbeitungsvorhaben oder bei Problemstellungen in der Datenbearbeitung einzubeziehen ist. Der Einbezug des Datenschutzberaters ist in Art. 10

Abs. 2 Bst. b nDSG bereits hinreichend normiert und es bedarf keiner Sonderregelung für eine spezifische Informationspflicht, die der Sache nicht dienlich ist. Unklar ist, was der Datenschutzberater mit dieser Meldung anfangen soll? Seine Funktion sollte nicht bürokratisiert werden, vielmehr sollte der die Fachanwender unterstützen.

Auch die DB des Bundesorgans hat bei der Anwendung der Datenschutzvorschriften mitzuwirken (vgl. Art. 28 E-VDSG). Es widerspricht dem präventiven und risikoorientierten Ansatz des rDSG, wenn die DB lediglich nachträglich über den Abschluss eines Outsourcingvertrags oder bei einer Funktionsübertragung informiert werden soll. Zu den Aufgaben der DB gehört die Involvierung in solche Geschäfte. Die ist eine Kernaufgabe der DB als Beratungsfunktion («Mitwirkung bei der Anwendung der Datenschutzvorschriften»). Die DB ist rechtzeitig zu informieren (und «mit ins Boot zu holen»), wie dies korrekterweise bei Datenbearbeitungsprojekten vorgesehen ist (Art. 31 E-VDSG). Um Kompetenz- und Umsetzungsfragen (vor allem auch der Praxis) bereits im Voraus verhindern zu können, raten wir Ihnen, diese Bestimmung und darin vor allem die Position der DB entsprechend der Definition im rDSG zu stärken.

Art. 8 E-VDSG (Beurteilung der Angemessenheit des Datenschutzes eines ausländisches Staates)
Bei den Formulierungen in dieser Bestimmung fällt auf, dass der EDÖB (formell) konsultiert wird, und die Beurteilungen von internationalen Organisationen oder ausländischen Behörden berücksichtigt werden können (materiell). Es ist klar zu formulieren, dass auch die Stellungnahmen des EDÖB materiell zu berücksichtigen sind, zumal sich die Erläuterungen hierzu nicht äussern (Erläuterungen, S. 27).

Art. 9 Abs. 3 E-VDSG (Datenschutzklauseln und spezifische Garantien)
Gemäss Art. 16 Abs. 2 Bst. b und c rDSG sind Datenschutzklauseln und spezifische Garantien dem EDÖB vorgängig mitzuteilen. Der Einleitungssatz von Art. 9 Abs. 3 E-VDSG suggeriert, dass es einen Sachverhalt geben könnte, in der auch die Nicht-Mitteilung zu einer rechtskonformen Bekanntgabe ins Ausland führen würde. Wir empfehlen, diese Formulierung entsprechend anzupassen.

Art. 13 E-VDSG (Modalitäten der Informationspflichten)
Diese Bestimmung ist unglücklich formuliert. Wer hat hier wen zu informieren? Geht es um die gegenseitigen Informationspflichten des verantwortlichen öffentlichen Organs und des Auftragsbearbeiters? Falls dem so ist, so ist die Kommunikation und Zusammenarbeit in differenzierter Form im jeweiligen Auftrag zu regeln und nicht abstrakt auf Verordnungsstufe und effektiven Normgehalt.

Art. 14 E-VDSG (Informationspflicht der Bundesorgane)
Die Informationspflichten sind auf Gesetzesstufe verankert. Deren Konkretisierung auf Verordnungsstufe dient dem Rechtsanwender kaum. Ein Beispiel: Während gemäss Art. 15 das verantwortliche öffentliche Organ und den Auftragsbearbeiter gleichermassen verpflichtet, dem Datenempfänger die einwandfreie Datenqualität zu bestätigen, ist in Art. 16 nur der Verantwortliche gehalten, den Datenempfänger über Berichtigungen, Einschränkungen, Vernichtungen und Löschungen von Personendaten zu informieren, dies aber unverzüglich, wobei unklar ist, was der Auftragsbearbeiter für eine Rolle hat.

Art. 18 E-VDSG (Form der Aufbewahrung der Datenschutz-Folgenabschätzung)
Diese Vorschrift geht unseres Erachtens fehl und verkennt das Instrument der Datenschutzfolgeabschätzung, welches dynamisch zu verstehen ist und während eines Projekts wie auch dessen Realisierung weiterentwickelt und den laufenden Erkenntnissen angepasst werden soll. Als amtliches Dokument, das auch Gegenstand der Vorabkonsultation beim Datenschutzaufsichtsorgan ist, unterliegt es den allgemeinen Regeln über die Aufbewahrungspflicht von Akten und nicht einer datenschutzrechtlichen Sonderlösung, welche der Funktion dieses wichtigen Datenschutzinstruments nicht gerecht wird.

Art. 19 E-VDSG (Meldung von Verletzungen der Datensicherheit)
Art. 24 Abs. 1 rDSG sieht eine Meldung von Verletzungen der Datensicherheit in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 rDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 rDSG).
Art. 24 rDSG ist eine (bewusst) abweichende Bestimmung von Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO aufgenommen. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen. Für die Mehrheit der Verantwortlichen trifft dies aber nicht zu. Art. 19 E-VDSG bringt somit unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht (die in der Praxis zudem möglichst rasch erfolgen soll) wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde rasch informiert wird, allenfalls auch die betroffenen Personen, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden. Es erscheint also fraglich, ob Art. 24 rDSG die in Art. 19 EVDSG enthaltene Konkretisierung überhaupt braucht.

Art. 20 E-VDSG (Auskunftsrecht – Modalitäten)
Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 rDSG definiert. Daraus ergeben sich Umfang und Zweck der Auskunft, was sich nach objektiven Kriterien misst. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte. Wir regen deshalb dazu an, Art. 20 Abs. 3 E-VDSG zu streichen.
Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen».
Dies ergibt sich bereits aus Art. 8 rDSG und den Bestimmungen des 1. Kapitels der E-VDSG, weshalb diese Bestimmung gestrichen werden kann und soll.
Art. 26 Abs. 4 rDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person. Deshalb ist Art. 20 Abs. 5 E-VDSG ersatzlos zu streichen.

Art. 25 E-VDSG (Besondere Bestimmungen – Datenschutzberater)
Art. 25 E-VDSG hält fest, welche Aufgaben die Datenschutzberater (DB) wahrnehmen muss. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 rDSG, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die er oder sie wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 rDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist missverständlich und entsprechend anzupassen. Dies könnte eventuell bereits mit dem Einfügen eines Passus wie «insbesondere» an geeigneter Stelle umgesetzt werden.

Art. 26 E-VDSG (Ausnahme von der Pflicht zur Führung eines Verzeichnisses)
In Anwendung von Art. 12 Abs. 5 rDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn

(1) umfangreich besonders schützenswerte Personendaten bearbeitet werden oder (2) ein Profiling mit hohem Risiko durchgeführt wird. Wie bei Art. 4 Abs. 1 E-VDSG ist zu erwähnen, dass diese Eingrenzung nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es unseres Erachtens angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 rDSG).

Art. 27 E-VDSG (Datenschutzberater – Ernennung)
Dass grundsätzlich jedes Bundesorgan einen Datenschutzberater zu ernennen hat ist unseres Erachtens übertrieben und unverhältnismässig. Das Schengener Datenschutzrecht verlangt den Einsatz von Datenschutzberatern nur in den Bereichen der Polizei, Strafverfolgung und Strafvollstreckung.

Art. 29 E-VDSG (Datenschutzberater – Pflichten des Bundesorgans)
Die Datenschutzberater sind keine ausgelagerten Funktionsträger des Datenschutzaufsichtsorgans, sondern interne Fachberater und Ansprechstellen für das Aufsichtsorgan wie auch das verantwortliche öffentliche Organ. Die Verankerung von umfassenden Einsichtsrechten können wir nicht unterstützen.

Art. 36 E-VDSG (Datenbearbeitung für nicht personenbezogene Zwecke)
Diese Bestimmung ist überflüssig, weil sich die darin enthaltene Präzisierung bereits aus Art. 39 rDSG ergibt.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und versichern Sie, Frau Bundesrätin, unserer vorzüglichen Hochachtung.

Im Namen des Regierungsrates:

Petra Steimen-Rickenbacher
Landammann

Regierungsrat Kanton Schwyz

Dr. Mathias E. Brun
Staatsschreiber

Der Regierungsrat des Kantons Thurgau

Thurgau

Staatskanzlei, Regierungsgebäude, 8510 Frauenfeld

Eidgenössisches
Justiz- und Polizeidepartement (EJPD)
Frau Karin Keller-Sutter
Bundesrätin
Bundeshaus West
3003 Bern

Frauenfeld, 28. September 2021
562

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Vernehmlassung

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Entwurf für eine Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11) und teilen Ihnen mit, dass wir mit der Vorlage grundsätzlich einverstanden sind. Für die weiteren Rechtssetzungsarbeiten bitten wir Sie indessen, die nachfolgenden Bemerkungen zu einzelnen Bestimmungen zu beachten.

Art. 2 E-VDSG

Die Aufzählung der Schutzziele ist zu kompliziert und sollte allgemeiner gehalten werden. Nach neuerer Definition beinhalten die Schutzziele meist die Vertraulichkeit, die Integrität der Daten, die Verfügbarkeit und die Nachvollziehbarkeit. Die im Entwurf gewählte Aufzählung ist zu detailliert und verkennt die neue Praxis bei Risikobeurteilungen.

Art. 3

In Art. 3 Abs. 4 des Entwurfs wird verlangt, dass die Protokolle der Datenbearbeitung „getrennt vom System, in dem die Personendaten bearbeitet werden, während zwei Jahren [besser: während zweier Jahre] aufzubewahren sind". Dies ist technisch praxisfremd. So werden heute die Protokolle jeweils automatisch von der laufenden Applikation im gleichen System erstellt und in den eigenen Verzeichnissen gespeichert. Müssen die Logdaten (Protokolle) in getrennte Systeme überführt werden, besteht die Gefahr, dass diese verändert werden. Kontrollen können dadurch zu falschen Ergebnissen führen. Die getrennte Aufbewahrung der Protokolle ist somit abzulehnen.

Regierungsgebäude, 8510 Frauenfeld
T +41 58 345 53 10, F +41 58 345 53 54
www.tg.ch

Art. 4

Der Bundesrat hat gestützt auf das revidierte Datenschutzgesetz keine Kompetenz, von Privaten die Erstellung eines Bearbeitungsreglements zu verlangen, zumal bei einer Bearbeitung mit hohen Risiken vorgängig gemäss Art. 22 des Datenschutzgesetzes vom 25. September 2020 (revDSG; BBL 2020 7639) eine Datenschutz-Folgenabschätzung mit diversen Dokumenten erstellt werden muss. Zusätzlich ein gesondertes Reglement zu verlangen, stellt einen unverhältnismässigen Aufwand für die Privatwirtschaft dar und schiesst am Ziel vorbei.

Im Weiteren ist nicht nachvollziehbar, weshalb gemäss Art. 4 Abs. 3 des Entwurfs das Reglement den Datenschutzberaterinnen und -beratern in einer Form zugestellt werden muss, die für diese verständlich sei, wenn diese Personen doch gemäss Art. 10 Abs. 3 lit. c revDSG über die erforderlichen Fachkenntnisse verfügen müssen. Auf die Pflicht zur Erstellung eines Bearbeitungsreglements ist zu verzichten.

Art. 6

Es ist zu begrüssen, dass eine beizuziehende Auftragsbearbeiterin oder ein solcher Auftragsbearbeiter einen gleichwertigen Datenschutz gewährleisten soll. Die Formulierung, wonach der Datenschutz andernfalls – also wenn das ausländische Gesetz den Datenschutz der Schweiz verletzt − auf vertraglichem Wege sicherzustellen sei, ist nicht nachvollziehbar und zu korrigieren.

So verlangen z.B. Art. 7 und 26 des chinesischen National Intelligence Law oder auch Title 18 Chapter 121 § 2713 des United States Code (US-CLOUD Act), dass die Anbieterinnen und Anbieter mit einem Bezug zu ihrem Land jede drahtgebundene oder elektronische Kommunikation sowie Aufzeichnungen oder sonstige Informationen, auch ausserhalb der eigenen Landesgrenzen liegend, den ausländischen Behörden offenlegen müssen. Dabei wird von der ausländischen Rechtsordnung bewusst eine Verletzung der schweizerischen Gesetzgebung in Kauf genommen (z.B. in § 2713 ii i.V.m. § 2703 1 A i CLOUD-Act). Auftragsbearbeiterinnen und -bearbeiter, die aufgrund ihres US- oder China-Bezugs derartigen Rechtspflichten unterstehen, können nicht mit einem Vertrag verpflichtet werden, schweizerische Daten sicher zu halten und die Vertraulichkeit einzuhalten. Dies ist ein absolutes Wunschdenken.

Zusammenfassend ist festzuhalten, dass der Datenschutz bei einem Auslandsbezug grundsätzlich durch Verträge oder Verfügungen sicherzustellen ist (analog zu § 12 des thurgauischen Gesetzes über den Datenschutz, TG DSG; RB 170.7). Ebenso ist betreffend Auslagerung von Daten zu beachten, dass bei einem Auslandsbezug mit tiefem Datenschutzniveau ein angemessener Datenschutz weder durch den Abschluss eines Vertrags noch mittels Verfügung erreicht werden kann. Es ist illusorisch, dass ausländisches Recht durch einen einfachen privatrechtlichen Vertrag ausgehebelt werden könnte.

Art. 15

Es mutet etwas seltsam an, dass eine private Unternehmung, die Personendaten weitergeben darf, die Empfängerin oder den Empfänger über die Zuverlässigkeit der eigenen Daten informieren muss.

Art. 20

Das Auskunftsrecht soll nach Art. 20 Abs. 1 des Entwurfs für die Gesuchstellerin oder den Gesuchsteller zukünftig etwas niederschwelliger ausgestaltet werden, indem das Auskunftsbegehren mit dem Einverständnis der verantwortlichen Person auch in mündlicher Form gestellt werden kann. Unseres Erachtens ist Schriftlichkeit jedoch zwingend nötig. Es sollte in jedem Fall immer ein schriftliches Auskunftsbegehren verlangt werden. Mündliche Auskunftsbegehren können zu Diskussionen und Missverständnissen führen und beinhalten somit ein Konfliktpotential. Wird die mündliche Form zugelassen, ist zudem zu befürchten, dass die Menge der Begehren zunimmt und letztere auch umfassender ausfallen, was den Bearbeitungsaufwand zusätzlich erhöht.

Art. 23

In Art. 2 der geltenden SR VSDG wird festgehalten, dass von einer Gesuchstellerin oder einem Gesuchsteller eine angemessene Kostenbeteiligung verlangt werden kann, wenn der antragstellenden Person in den zwölf Monaten vor dem Gesuch die gewünschten Auskünfte bereits mitgeteilt wurden und kein schutzwürdiges Interesse an einer neuen Auskunftserteilung nachgewiesen werden kann. Diese Regelung hat sich bewährt. Leider ist sie im nun vorliegenden Verordnungsentwurf weggefallen, wodurch die praktische Umsetzung der Kostenfrage erschwert wird. Diese Regelung sollte beibehalten werden.

Art. 28

Gemäss Art. 10 Abs. 2 lit. b revDSG haben Datenschutzberaterinnen und -berater eines Bundesorgans bei der Anwendung der Datenschutzvorschriften mitzuwirken, was bei der Auflistung der Aufgaben in Art. 28 Abs. 2 des Entwurfs vergessen gegangen ist und korrigiert werden sollte.

Mit freundlichen Grüssen

Die Präsidentin des Regierungsrates

Der Staatsschreiber

DER REGIERUNGSRAT · DES KANTONS THURGAU ·

Numero			Bellinzona
5144	fr	0	20 ottobre 2021

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Dipartimento federale giustizia e polizia
3003 Berna

jonas.amstutz@bj.admin.ch

Revisione totale dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD) – Procedura di consultazione

Signora Consigliera federale,
gentili signore,
egregi signori,

ringraziandovi per averci coinvolto nella procedura di consultazione in oggetto, vi comunichiamo che non abbiamo evidenziato particolari criticità, per cui rinunciamo a formulare delle riserve.

Vogliate gradire, signora Consigliera federale, signore e signori, l'espressione della nostra alta stima.

PER IL CONSIGLIO DI STATO

Il Presidente — Manuele Bertoli

Il Cancelliere — Arnoldo Coduri

Copia a:
- Servizi giuridici del Consiglio di Stato (can-cgcs@ti.ch)
- Incaricato cantonale della protezione dei dati (giordano.costa@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in Internet

Landammann und Regierungsrat des Kantons Uri

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassung

Sehr geehrter Herr Direktor
Sehr geehrte Damen und Herren

Am 23. Juni 2021 hat das Eidgenössische Justiz- und Polizeidepartement (EJPD) im Rahmen eines Vernehmlassungsverfahrens die Kantonsregierungen eingeladen, zur geplanten Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellung zu nehmen. Wir äussern uns dazu wie folgt:

Wie beim Eidgenössischen Datenschutzgesetz (DSG) umfasst auch der Geltungsbereich der VDSG lediglich die Datenbearbeitung durch Private und durch Bundesorgane. Der Kanton ist von der Regelung deshalb nicht unmittelbar betroffen. Einige Berührungspunkte ergeben sich jedoch dennoch.

Diese Vernehmlassungsvorlage beschränkt sich nicht nur auf jene Regelungen, zu denen der Bundesrat im DSG ermächtigt wird, sondern geht darüber hinaus. Dabei sind manche zusätzlichen Regeln eher trivial, um nicht zu sagen unnötig. Andere enthalten konkrete Pflichten, bei denen nicht durchwegs klar ist, ob und auf welche Grundlage auf Gesetzesstufe sie sich abstützen. Die Anforderungen an die Datensicherheit wiederum, die gemäss Vorgabe des DSG lediglich Mindestanforderungen sind, sind enorm. Natürlich entsprechen die gesteigerten Anforderungen an Datenschutz und Datensicherheit der Stossrichtung des DSG und auch den internationalen Anforderungen. Dennoch stellt sich die Frage, ob und zu welchem Preis insbesondere KMU diesen Anforderungen gerecht werden können.

Bemerkungen zu einzelnen Bestimmungen:

Zu Artikel 4

Diese Bestimmung schreibt vor, dass private Verantwortliche oder deren Auftragsbearbeiter, sofern sie in grossem Ausmass besonders schützenswerte Personendaten bearbeiten oder ein Profiling mit hohem Risiko erstellen, ein Bearbeitungsreglement zu verfassen haben. Allerdings reichen diese Voraussetzungen aus datenschutzrechtlichen Überlegungen nicht aus. Der Bereich kritischer Datenbearbeitung erweist sich als umfassender, weswegen die Eingrenzung auf die im Entwurf erwähnten Vorgaben als zu eng erscheint. Eine Möglichkeit ergäbe sich, die Voraussetzungen, die für die Datenschutz-Folgeabschätzung vorgesehen sind, zu übernehmen (Datenbearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen). Im Rahmen einer Datenschutz-Folgeabschätzung werden überdies zahlreiche Dokumente erstellt, die Teil des in Artikel 4 vorgesehenen Bearbeitungsreglements sein könnten.

Absatz 3 vermittelt eher den Eindruck, dass diese Bestimmung nicht der Praxis gerecht werden kann. Hält man sich vor Augen, welche Voraussetzungen und Aufgaben eine Datenschutzberaterin oder ein Datenschutzberater gemäss Artikel 28 Verordnungsentwurfs erledigen muss, dann erscheint es kaum realistisch, dass seitens des privaten Verantwortlichen das Reglement den beratenden Fachpersonen in einer für diese verständliche Sprache zur Verfügung gestellt wird. Vielmehr gehört es zu den Aufgaben der Datenschutzberaterinnen und Datenschutzberater, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b revDSG), überdies haben diese Fachpersonen über die erforderlichen Fachkenntnisse zu verfügen (Art. 10 Abs. 3 Bst. c revDSG).

Zu Artikel 7

Wie bereits erwähnt, haben die Datenschutzberaterinnen und Datenschutzberater der privaten Verantwortlichen, so auch jene der Bundesorgane, bei der Anwendung von Datenschutzvorschriften mitzuwirken. Dieser Mitwirkungspflicht, welche im revDSG vorgesehen ist, kommt eine präventive Bedeutung zu, welche vernachlässigt würde, wenn der zuständige Verantwortliche die Datenschutzberaterin oder den Datenschutzberater erst nach vollzogenem Rechtsgeschäft über den Abschluss eines Outsourcingvertrags orientieren muss. Diese fachlichen Beratungspersonen sollten zum Voraus rechtzeitig informiert werden, wie dies beispielsweise auch bei Datenbearbeitungsprojekten vorgesehen ist (Art. 31), damit die Beratung auch rechtzeitig stattfinden kann.

Zu Artikel 19

Artikel 24 Absatz 1 revDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führen können. In Artikel 24 Absatz 2 revDSG wird der Inhalt der Meldung präzisiert. In den Absätzen 4 und 5 derselben Bestimmung werden die Voraussetzungen einer solchen Information festgelegt.

Mit der Formulierung von Artikel 24 revDSG wollte man teilweise bewusst von Artikel 33 DSGVO der

EU abweichen. Dennoch wird nun in Artikel 19 des Verordnungsentwurfs mehrheitlich die Bestimmung von Artikel 33 DSGVO übernommen. Das mag zwar solchen Verantwortlichen dienen, die auch der DSGVO unterliegen (international tätige Firmen), für die grosse Mehrheit der Verantwortlichen in der Schweiz ist dies jedoch kaum der Fall. Daher sind in der entworfenen Verordnungsbestimmung zusätzliche Bestimmungen aufgeführt, die so nicht als notwendig erscheinen.

Zu Artikel 20

Artikel 25 und 26 revDSG regeln das Auskunftsrecht von betroffenen Personen und dessen Einschränkungen relativ eingehend. In Artikel 20 des Verordnungsentwurfs sind teilweise Regelungen enthalten, bei denen man sich fragen kann, ob diese zusätzlich als notwendig erscheinen. So ist in Artikel 20 Absatz 3 festgehalten, dass die Auskunft für die betroffene Person verständlich sein muss. Das könnte missverstanden werden. Der Inhalt der Auskunft ist in Artikel 25 Absatz 2 revDSG klar umschrieben. Umfang und Zweck lassen sich daraus in objektiver Weise ableiten. Artikel 20 Absatz 3 schafft mehr Unsicherheit als Klarheit für Verantwortliche, da eigentlich in Artikel 25 Absatz 2 revDSG der objektive Inhalt einer Auskunft klar vorgegeben ist.

Zu Artikel 21

Diese Bestimmung sieht vor, dass ein Verantwortlicher, der für die Behandlung des Auskunftsbegehrens nicht persönlich zuständig ist, dieses an den zuständigen Verantwortlichen weiterleiten muss. Das ist, soweit es den öffentlich-rechtlichen Verwaltungsbereich betrifft, eigentlich eine Selbstverständlichkeit, handelt es sich doch um einen verwaltungsrechtlichen Grundsatz.

Zu Artikel 25

In der entworfenen Bestimmung ist der Aufgabenbereich der Datenschutzberaterinnen und Datenschutzberater festgehalten. Es wird dabei aber nicht Bezug genommen zu Artikel 10 Absatz 2 revDSG, wo insbesondere zwei Aufgabenbereiche festgehalten sind, nämlich die Schulung und Beratung sowie die Mitwirkung bei der Anwendung von Datenschutzvorschriften. Dieser Aufgabenbereich ist letztlich sehr umfassend, weshalb die «Aufgaben» in Absatz 1 Buchstabe a und b nicht die eigentlichen Aufgaben sind, welche die fachlichen Beratungspersonen wahrnehmen müssen, sondern lediglich nicht abschliessende Beispiele von Konkretisierungen der im Gesetz (Art. 10 Abs. 2 revDSG) festgeschriebenen Aufgaben.

Sehr geehrter Herr Direktor, sehr geehrte Damen und Herren, wir danken Ihnen für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 1. Oktober 2021

REGIERUNGSRAT DES KANTONS URI

Im Namen des Regierungsrats

Der Landammann — Urban Camenzind

Der Kanzleidirektor — Roman Balli

canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Madame la Conseillère fédérale
Karin Keller-Sutter
Cheffe du Département fédéral de justice
et police (DFJP)
3003 Berne

Par courrier électronique à :
jonas.amstutz@bj.admin.ch

Réf. : 21_COU_7296

Lausanne, le 13 octobre 2021

Réponse du Canton de Vaud à la consultation fédérale sur le projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (P-OLPD)

Madame la Conseillère fédérale,

Le Conseil d'Etat a pris connaissance du projet de révision totale de l'ordonnance relative à la loi fédérale du 15 septembre 2020 sur la protection des données et vous remercie de l'avoir consulté à ce sujet.

Convaincu de la nécessité impérieuse de protéger les personnes, les entreprises et autres collectivités des risques découlant d'une utilisation abusive de leurs données, ainsi qu'il l'a affirmé dans sa Stratégie numérique de novembre 2018, le Conseil d'Etat ne saurait, en l'état, soutenir le projet de révision mis en consultation, dès lors que bon nombre de ses dispositions et notamment celles qui portent sur la sécurité des données, manquent à ce stade de la clarté qui permettrait aux responsables privés ou fédéraux de traitement des données de les mettre en œuvre. Dans ce contexte, le Conseil d'Etat note qu'à ce stade, le projet de révision reprend des termes et dispositions obsolètes de l'ordonnance fédérale précédente, et, de manière partielle, certaines dispositions du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), ne permettant pas d'en saisir la finalité.

Pour le Conseil d'Etat, il est indispensable que la future ordonnance soit précise car la loi fédérale est complexe, contient de nombreuses normes de délégation, et introduit des concepts nouveaux tels que celui du profilage à risque élevé (article 5 let g nLPD). Le Conseil d'Etat est d'ailleurs d'avis que toute forme de profilage est en soi un traitement de données à risque élevé, susceptible de porter atteinte à la personnalité ou aux droits fondamentaux d'une personne. Enfin, le Conseil d'Etat rappelle que la nLPD et l'OLPD serviront de référence au droit cantonal de la protection des données que les cantons devront réviser notamment pour tenir compte des évolutions sociétales et techniques, ainsi que de certaines dispositions du droit européen – il est dès lors essentiel que le droit fédéral soit précis.

Le Conseil d'Etat demande ainsi au Conseil fédéral de clarifier le projet de révision, en tenant compte de ses commentaires figurant en annexe.

En vous remerciant de l'attention que vous porterez à la présente détermination, le Conseil d'Etat vous prie de croire, Madame la Conseillère fédérale, à l'assurance de sa haute considération.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LA CHANCELIERE a.i.
Nuria Gorrite	Sandra Nicollier

Annexe mentionnée

Copies

- Autorité de protection des données et de droit à l'information
- Office des affaires extérieures

Annexe

Commentaires article par article :

Section 1 sécurité des données

D'une manière générale, le P-OLPD ne précise pas suffisamment les exigences minimales en matière de sécurité des données (art. 8 nLPD) et ne permet pasde reconnaitre les éléments objectifs de l'infraction relative à la violation des devoirs de diligence (art. 61 al. 1 let. c nLPD).

En effet, le P-OLPD s'en tient au concept de l'ordonnance précédente et le complète par des termes de droit européen, sans préciser la nécessité d'adapter les mesures visant à sécuriser les données à la finalité de leur traitement ainsi qu'aux outils utilisés. Dans ce contexte, il pourrait être pertinent de prévoir de se référer à des normes techniques et organisationnelles internationalement reconnues, qui permettraient de tenir compte des évolutions technologiques.

Il serait également nécessaire par ailleurs de fixer dans cette section des critères indiquant la pertinence voire l'obligation de conduire des analyses d'impact de protection des données (DPIA). En effet, il s'agit de concrétiser et développer la notion de « risque accru pour la personnalité et les droits fondamentaux de la personne concernée » de l'art. 16 al. 1 LPD.

Article 1

L'al. 1 semble reprendre pour l'essentiel l'art. 32 du RGPD sans toutefois se concentrer sur l'objectif formulé dans cet article, à savoir : « assurer un niveau de protection adapté au risque ». Cela signifie, qu'en fonction des cas, il conviendra au préalable d'évaluer les objectifs, les besoins et les risques en matière de protection des données. A ce sujet, les objectifs de protection sont déjà fixés à l'art. 5 al. 1 let. h nLPD, comme le mentionnent également les notes explicatives (p. 15 du rapport), et sont énumérés en détail à l'art. 2 P-OLPD (voir ci-dessous art. 2 P-OLPD). Le besoin de protection est déterminé par le type de données (données personnelles, données personnelles sensibles) et le traitement des données en lui-même (par exemple, le profilage). Ce n'est qu'ensuite qu'aura lieu l'évaluation des risques, comme le prévoit également l'analyse d'impact sur la protection des données (art. 22 nLPD).
Les critères « finalité, nature, étendue et circonstances du traitement des données » se réfèrent ainsi à l'évaluation du besoin de protection (qui contient déjà une première estimation approximative de l'étendue possible du dommage), les critères « probabilité de survenance et d'impact potentiel sur les personnes concernées » à l'évaluation des risques. Lorsqu'il s'agit d'évaluer l'adéquation des mesures, les critères « état de la technique et coûts de mise en œuvre » semblent pertinents. Toutefois, ils ne renseignent qu'indirectement sur l'opportunité d'une mesure, car en ce qui concerne cette dernière, il faut avant tout permettre d'évaluer si une mesure doit être prise et, concrètement, laquelle permet de contrer le risque de manière adéquate (cf. art. 32 RGPD et notes explicatives, p. 15).

L'art. 1 al. 1 P-OLPD devrait donc être entièrement revu sur le plan conceptuel et il serait judicieux d'ajouter, à la lettre a) les critères de **profilage**, de **transferts internationaux** et de **sous-traitance** (Cloud). Ces situations sont particulièrement critiques en matière de gestion des risques, tant pour les personnes physiques que morales.

L'al. 2 exige que les mesures soient examinées à intervalles appropriés pendant toute la durée du traitement. Cette formulation apparaît insuffisante en ce sens que l'évaluation des risques dont découle les mesures et leur pertinence, doit être revue en permanence et par conséquent induire l'adaptation éventuelle des mesures. Cet alinéa devrait être reformuler afin de garantir une sécurité suffisante des données.

Le Conseil d'Etat propose d'ajouter à cet article un troisième alinéa ayant la teneur suivante :

Art. 1, al. 3 [Nouveau] *: « Le PFPDT publie des recommandations sur les mesures techniques et organisationnelles que le responsable du traitement et les sous-traitants peuvent envisager selon la nature des données personnelles traitées »*.

En effet, l'élaboration de « recommandations de bonne pratique », sous l'égide du PFPDT, sur les moyens que le responsable du traitement peut mettre en œuvre, avec des exemples concrets d'application (p. ex. dans le domaine médical) pourrait servir de référence aux exigences à remplir et à l'évaluation cas échéant (p. ex. les autorités de surveillance ou la justice). Cette proposition va également dans le sens du Commentaire § 4.1.1 « Sécurité des données » p. 14, troisième paragraphe, qui précise : « En toute logique, les exigences sont plus élevées pour un hôpital qui traite régulièrement des données sensibles que pour une boulangerie ou une boucherie qui traite les données de ses clients ou de ses fournisseurs. »

Article 2

Les exigences énumérées ne représentent pas des objectifs de protection indépendants, mais plutôt des exigences relatives aux mesures à prendre pour atteindre les objectifs de protection (par exemple, le contrôle d'accès ne représente pas un objectif de protection, mais plutôt une exigence visant à garantir la confidentialité dans le cadre du principe de proportionnalité). Si l'art. 5 al. 1 let h nLPD énumère ces objectifs de protection, il serait opportun de les détailler plus clairement dans l'ordonnance d'application tout en actualisant et harmonisant les termes.
En outre, il conviendrait de préciser dans la phrase introductive de l'art. 2 que les mesures devraient être définies en tenant compte des risques identifiés lors de l'évaluation des risques, et porter sur les éléments listés dans l'article.

Article 3

L'objectif de la journalisation est que, dans les cas où le traitement non autorisé de données personnelles ne peut pas être techniquement exclu dès le départ, il puisse être ultérieurement déterminé (et sanctionné dans certaines circonstances par la suite) lors de l'analyse du journal. La journalisation résulte donc de l'évaluation des risques et de la planification des mesures. Il doit s'agir d'un moyen approprié au regard d'un risque concret

qui peut être efficacement réduit par la journalisation (proportionnalité du nouveau traitement des données). L'obligation de journalisation des données en tant que mesure compensatoire ne devrait donc s'appliquer que dans les cas où elle répond effectivement à un risque identifié.

L'al. 2 prévoit que pour les organes fédéraux, la journalisation doit s'appliquer au traitement de toutes les données personnelles. Cette mesure paraît aller trop loin, et être trop contraignante. La journalisation constitue en soi une acquisition de données personnelles, qui doit satisfaire au principe de proportionnalité. Il est vrai que l'art. 57 let. b ch. 4 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA) permet l'enregistrement de données marginales dans le but de tracer l'accès aux collections de données, mais seulement dans la mesure où l'enregistrement est proportionné. Le fait que, même dans le cas de données personnelles simples et même avec des autorisations restrictives, chaque accès en lecture doive être enregistré va clairement au-delà de cette exigence. L'obligation des organes fédéraux de « journaliser » ne doit pas aller plus loin que celle des personnes privées responsables du traitement. Il conviendrait donc d'inclure les organes fédéraux dans l'al. 1 et de supprimer l'al. 2.

Al. 3, il convient d'insérer les mots "**le cas échéant**" avant "l'identité du destinataire", car tout traitement enregistré ne constitue pas une divulgation.

Al. 4, les journaux doivent être conservés pendant deux ans et ne peuvent être utilisés que pour contrôler les règles de protection des données ou pour rétablir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données. Dans ce contexte, une évaluation liée à la personne n'est pas nécessaire dans tous les cas (cf. art. 57m et suivants LOGA et ATF 143 II 443 qui précisent les modalités des évaluations et des procédures échelonnées) pour les organes fédéraux. Il convient donc de modifier la dernière phrase comme suit : « **ne peuvent être utilisés qu'à cette fin et dans la mesure nécessaire à l'égard des personnes** ».

Article 4

Avec cette nouvelle norme, la protection des particuliers s'amoindrit. En effet, l'al. 1 restreint de façon arbitraire l'obligation de créer un règlement de traitement pour les responsables privés et leurs sous-traitants mandatés. Cette solution limitée à deux cas de figure ne permet plus de garantir les droits de la personne concernée dans le traitement de ses données.
Il convient ici de reprendre les exigences de l'analyse d'impact sur la protection des données (cf. art. 22 al. 1 nLPD). Dans le cadre de l'analyse d'impact sur la protection des données, de nombreux documents sont également créés (art. 22 al. 3 nLPD), qui peuvent faire partie du règlement de traitement. Les recommandations de bonne pratique évoquées plus haut permettraient également de garantir un cadre sécuritaire dès que le traitement porte sur des données sensibles que ce soit à grande échelle ou non.

L'al. 2 n'établit aucun lien avec les normes en matière de technologie de l'information auxquelles il conviendrait de se référer. Une solution simple serait de se référer aux exigences spécifiques de la protection des données (let. h, j).

L'al. 3 semble peu pratique. Le conseiller à la protection des données est le spécialiste du responsable du traitement et c'est lui qui élabore un ensemble de règles de traitement et veillera également à son actualisation cas échéant. La formulation « le met à la disposition du conseiller à la protection des données sous une forme qui lui est intelligible » implique manifestement une dévalorisation des compétences spécialisées requises (art. 10 al. 3 let. c nLPD). L'une des tâches du conseiller à la protection des données est d'aider à l'application de la réglementation en matière de protection des données (art. 10 al. 2 let. b nLPD). L'al. 3 P-OLPD devrait être supprimé sans être remplacé.

Article 5

cf. commentaire article 4.

Article 6

Correction d'une coquille à l'al. 3 « Lorsque le responsable **du** traitement … ».

Article 7

Le conseiller à la protection des données de l'organe fédéral doit également collaborer à l'application des dispositions relatives à la protection des données (cf. ci-dessous art. 28 P-OLPD). Il est contraire à l'approche préventive et axée sur les risques de la nLPD que le conseiller à la protection des données ne soit informé qu'a posteriori de la conclusion d'un contrat d'externalisation ou en cas de transfert de fonctions. Les tâches d'un conseiller en protection des données incluent la participation à de telles transactions ; il s'agit d'une tâche essentielle et le conseiller à la protection des données doit être informé en temps utile, comme cela est prévu lors de la conception de projets de traitement automatisé de données personnelles (art. 31 P-OLPD). L'art. 7 P-OLPD devrait être supprimé sans être remplacé.

Article 8

La mise en application de cet article impliquerait que le PFPDT soit consulté formellement alors que les appréciations des organisations internationales ou des autorités étrangères peuvent quant à elles être prises en compte matériellement. Il convient donc de préciser que les avis du PFPDT sont également à prendre en compte sur le plan matériel, d'autant que les notes explicatives ne se prononcent pas à ce sujet (notes explicatives, p. 27).

Article 9

En vertu de l'art. 16 al. 2 let. b et c nLPD, les clauses de protection des données et les garanties spécifiques doivent être communiquées préalablement au PFPDT. La formulation introductive de l'al. 3 pourrait laisser penser que l'absence de communication, dans certains cas, constituerait également une divulgation conforme à la loi à l'étranger. Il convient de souligner que dans le contexte du RGPD et des traitements et transferts entre personnes morales d'une même entité ou appartenant au même groupe, ces dernières doivent être considérées comme tierces parties. Dès lors, un contrat de sous-traitance et des clauses de protection sont exigés. La formulation devrait être adaptée afin de lever toute ambiguïté.

Article 13

. L'article 13 pourrait préciser qui est responsable au premier chef de la communication sur le traitement de données entre le responsable de traitement et le sous-traitant, en garantissant une bonne coordination ainsi qu'une information uniforme et valable à la personne concernée.

Article 19

L'art. 24 al. 1 nLPD prévoit la notification des violations de sécurité des données uniquement dans les cas susceptibles d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. L'art. 24 al. 2 nLPD précise le contenu de la notification et énonce les exigences relatives à l'information des personnes concernées (art. 24 al. 4 et 5 nLPD).

L'art. 24nNLPD diverge de l'art. 33 RGPD ; cependant, la majorité des dispositions de l'art. 33 RGPD sont reprises pour l'essentiel dans l'art. 19 P-OLPD. Si ces dispositions sont utiles pour les contrôleurs qui sont également soumis au RGPD, ce n'est pas le cas pour la majorité des responsables du traitement. Cet article introduit des dispositions supplémentaires inutiles, souvent limitées par la formulation « dans la mesure du possible ». L'art. 24 nLPD n'a pas besoin de la concrétisation contenue dans l'art. 19 P-OLPD.

Article 20

Les art. 25 et 26 nLPD réglementent en détail le droit à l'information et ses restrictions ; les précisions fournies par l'art. 20 P-OLPD vont au-delà de ce qui est nécessaire.

L'al. 3 précise que les renseignements doivent être compréhensibles pour la personne concernée ; cette formulation est trompeuse car elle impliquerait que le responsable du traitement devrait traiter des données supplémentaires sur la personne qui demande des informations afin d'établir avec certitude sa bonne compréhension. Or le contenu de l'information est défini à l'art. 25 al. 2 nLPD qui détermine la portée et le but de l'information, mesuré selon des critères objectifs. Il importe que le droit à l'information puisse être intégré dans les processus du responsable du traitement comme une norme évidente de la loi sur la protection des données. L'art. 20 al. 3 P-OLPD devrait être supprimé sans être remplacé.

L'al. 4 rappelle inutilement l'obligation pour les responsables du traitement de « protéger les données de la personne concernée de tout accès de tiers non autorisé lors de la communication des renseignements ». Cette obligation découle déjà de l'art. 8 nLPD et des dispositions du chapitre 1 de P-OLPD. L'al. 4 P-OLPD devrait être modifié en ce sens.

L'al. 5 oblige le responsable du traitement à documenter la restriction et conserver cette documentation pendant au moins trois ans. Cette nouvelle obligation crée un travail supplémentaire sans garantie sur la suite donnée ni cadre précis sur la durée de conservation de ces informations partielles. Selon l'art. 26 al. 4 nLPD le responsable du traitement doit indiquer pourquoi il refuse, restreint ou reporte l'information ; cette disposition est suffisante pour que la personne concernée puisse faire valoir son droit à

l'information en justice si nécessaire. L'al. 5 P-OLPD devrait être supprimé sans être remplacé.

Article 21

L'al. 1 prévoit que le responsable du traitement qui n'est pas compétent pour traiter la demande doit la transmettre au responsable du traitement compétent. Ce principe de droit administratif s'applique aux organes fédéraux même sans être mentionné dans ce contexte. Si dans le domaine du droit public, cette obligation résulte de la relation souveraine des citoyens avec l'État, dans la relation de droit privé, en revanche, les parties déterminent leurs droits et obligations de manière autonome. Il est disproportionné d'imposer la même obligation à la personne responsable de droit privé. Elle conduit à un effort de recherche de la personne « responsable » en droit privé sans renforcer les droits des personnes concernées. L'al. 1 2ème phrase P-OLPD devrait être supprimé sans être remplacé.

Article 23

Cette disposition pourrait être complétée par un renvoi aux dispositions topiques de la législation sur la protection des données régissant la procédure à suivre lorsque la personne concernée conteste l'émolument demandé car, contrairement à l'organe saisi, elle estimerait par exemple que les efforts à déployer pour répondre à sa demande ne seraient pas disproportionnés.

Article 24

Se référer à l'application analogue des dispositions sur le droit d'accès pour la mise en œuvre de l'art. 28 nLPD ne rend pas justice à la nouvelle institution juridique de la « portabilité des données » et ne répond pas à la nécessité de la concrétiser. Il serait judicieux de traiter ici notamment des « formats électroniques communs » ou de « l'effort disproportionné » en cas de transfert direct d'un contrôleur de données à un autre. En outre, en ce qui concerne les exceptions de gratuité, une réglementation différente de celle du droit à l'information serait également concevable, car ici ce n'est pas la protection de la personnalité mais la valeur économique des données qui est au premier plan. L'art. 24 P-OLPD devrait ainsi être complètement révisé.

Article 25

La formulation de cet article paraît trompeuse et devrait être corrigée. En effet, aucune référence n'est faite à l'art. 10 al. 2 nLPD, qui énumère deux tâches du conseiller à la protection des données en particulier : la formation et le conseil ainsi que la participation à l'application des règles de protection des données. Ces obligations légales sont exhaustives, c'est pourquoi les obligations de l'art. 25 al. 1 let a et b P-OLPD ne sont pas les obligations que ce conseiller doit remplir, mais une simple concrétisation des obligations déjà énoncées à l'art. 10 al. 2 nLPD.

Article 26

Restreindre l'obligation de tenir un registre des activités de traitement qu'à deux situations très précises ne couvre pas les traitements de données qui sont essentiels pour les droits de la personne. Comme dans le cas de l'art. 4 al. 1 P-OLPD, ici aussi, il convient de reprendre les exigences relatives à l'analyse d'impact sur la protection des données (le traitement comporte un risque élevé pour la personnalité et les droits fondamentaux des personnes concernées ; art. 22 al. 1 nLPD).

Article 28

L'al. 2 omet de reprendre la tâche prévue à l'art. 10 al. 2 let. b nLPD – concourir à l'application des prescriptions relatives à la protection des données – seule figure la formation et le conseil de l'art. 10 al. 2 let. a nLPD. Il s'agit probablement d'un oubli, puisque la participation à l'application des réglementations en matière de protection des données est une tâche essentielle des conseillers à la protection des données. Cette tâche devrait ainsi être ajoutée à l'art. 28 al. 2 P-OLPD.

Article 33

Cette disposition devrait être complétée de manière à prévoir une obligation de consulter les autorités cantonales lorsque les projets les impliquent également.

Article 36

La disposition est superflue car cette spécification est déjà claire à partir de l'art. 39 nLPD.

Annexe relative à la modification de l'Ordonnance sur les relevés statistiques
Liste des statistiques (Ch. 72, titre, 3e ligne, 2e colonne, et 9e ligne, 2e colonne)

Il ressort de ce descriptif qu'« avec l'accord des intéressés, il est possible d'utiliser certaines informations dans certains buts administratifs », ce qui figure déjà à l'annexe de l'ordonnance actuelle sur les relevés statistiques.
Or, cette possibilité est une dérogation importante aux principes régissant les traitements de données statistiques, il est proposé de compléter par des exemples, ce que l'on entend par « dans certains buts administratifs », avec la mention « notamment » ou « tels »…

Traitement de données sensibles

Le Conseil d'Etat relève que le traitement de données sensibles devrait, selon la nLPD être prévu au niveau d'une base légale formelle. Or on peut constater dans les textes mis en consultation, l'introduction de normes autorisant le traitement de données sensibles. Ces dispositions devraient être retirées du projet de révision et être soumises dans un projet de loi aux Chambres fédérales.

Propositions rédactionnelles :

- No 109 (ordonnance sur le travail au noir), changer le titre de l'article 9a : « ~~Protection des données personnelles~~ **Données des personnes morales** » ;

- No 112 (ordonnance sur le service civil), article 110 al. 1 « Le CIVI **est** une banque de données… » ;

- No 116 (OAMal), art. 59a al. 1 in fine : « Le DFI fixe **au niveau suisse** la structure uniforme des ensembles de données » ;

- Art. 59a al. 7 in fine : « Il publie une liste des services **certifiés** de réception des données. ».

* * *

Conseil d'Etat
Staatsrat
CP 478, 1951 Sion
CANTON DU VALAIS
KANTON WALLIS

2021.04341

P.P. CH-1951 Sion
Poste CH SA

Département fédéral de justice et police
Madame Simonetta Sommaruga
Conseillère fédérale
Palais fédéral
3003 Berne

Notre réf. /
Votre réf. /

Date 13 octobre 2021

Avant-projet de l'Ordonnance relative à la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales
Procédure de consultation

Madame la Conseillère fédérale,

Le Conseil d'Etat du canton du Valais vous remercie de l'avoir consulté à propos de la révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD).

Au titre des nouveautés, la révision totale de l'OLPD propose notamment de préciser les critères à prendre en compte dans le cadre d'une approche fondée sur le risque et de fournir une ligne directrice quant à la façon de concevoir les mesures, tant au niveau des organes fédéraux qu'au niveau des personnes privées, en dressant une liste d'objectifs de protection. Le projet de révision revoit entièrement la section portant sur la communication de données personnelles à l'étranger, en garantissant un niveau de protection approprié. Sont également prévus un droit d'accès facilité aux requérants et la suppression de la consultation de données d'une personne décédée.

Le Conseil d'Etat du canton du Valais note avec satisfaction que les objectifs poursuivis par la révision totale de l'OLPD résident notamment dans une lecture plus claire et structurée de l'ordonnance, ainsi que dans un complément en matière de sécurité des données, afin particulièrement de garantir une compatibilité entre les dispositions fédérales, d'une part, et le règlement européen de protection des données (RGPD) et la directive (UE) 2016/680 applicable à la Suisse, d'autre part. Cela étant, il apparaît que, dans plusieurs dispositions, des termes obsolètes sont repris de l'ordonnance actuelle et complétés par des termes du droit européen, sans pour autant avoir été adaptés et revus conceptuellement (cf. par ex. art. 1 Avant-projet OLPD par rapport à l'art. 32 RGPD), que plusieurs dispositions manquent de clarté en vue de leur mise en œuvre correcte par les différents responsables du traitement des fichiers (cf. par ex. art. 2 [objectifs de protection devant être reformulés de manière compréhensible], 4, 5 et 20 al. 3 [notions arbitraires et/ou subjectives utilisées]) et que l'avant-projet contient certaines redites (not. art. 20 al. 4 par rapport au Chapitre 1 de l'avant-projet et à l'art. 8 pLPD, art. 25 par rapport à l'art. 10 al. 2 pLPD et art. 29 par rapport à l'art. 39 pLPD).

Dans l'ensemble, la recherche de conciliation du droit fédéral avec le droit européen se doit d'être saluée au terme du projet relatif à la révision totale de la LPD et de l'OLPD. En effet, il apparaît essentiel à l'heure actuelle pour la Suisse d'intégrer les normes européennes à sa législation et d'en respecter, à tout le moins, les conditions et règles minimales. A l'heure de la complexification et de l'importante codification en matière de protection des données, les entreprises dont le siège se trouve en Suisse pourront ainsi se voir reconnues et respectées au niveau européen et mondial,

s'agissant notamment du niveau de protection adéquat garanti. Parallèlement, l'édition d'une annexe, mise à jour régulièrement en particulier suite aux ratifications de la Convention 108+, comprenant les Etats, territoires, secteurs déterminés dans un Etat et organismes internationaux dans lesquels un niveau de protection adéquat est garanti apparaît présentement nécessaire et bienvenue.

L'avant-projet de l'ordonnance prévoit les exigences minimales à respecter s'agissant de la sécurité des données comme « lignes directrices », tout en laissant une certaine souplesse aux concernés, dès lors que tant la loi que l'ordonnance suivent une approche fondée sur le risque et qu'il serait impossible de définir des exigences minimales générales applicables à chaque branche. Dans cette optique, le Conseil d'Etat observe et reconnaît un but de conscientisation et de responsabilisation du responsable du traitement des fichiers.

La révision totale de l'OLPD vise, au final, une meilleure mise en œuvre de la nouvelle LPD et une codification plus systématique. Elle permettra également d'asseoir nombre de principes déjà encrés en cette matière et de les préciser. Elle n'aura que peu de conséquences financières et apportera avec certitude une meilleure protection des données en règle générale. Cela étant, comme indiqué *supra*, quelques travaux de conceptualisation et de clarification méritent encore d'être effectués. De ce fait, et compte tenu des remarques formulées, le Gouvernement valaisan accueille favorablement les modifications de l'ordonnance de mise en application de la législation fédérale en matière de protection des données.

En 2008, le canton du Valais s'était doté de sa propre loi sur l'information du public, la protection des données et l'archivage (LIPDA), laquelle est en vigueur depuis 2011. Le canton du Valais est occupé à réviser la LIPDA en prévoyant une mise à jour générale des dispositions en matière de protection des données pour tenir compte des modifications et développements législatifs importants en la matière survenant tant au niveau fédéral qu'international.

Le Conseil d'Etat du canton du Valais vous remercie de l'avoir consulté sur cette question et vous prie de croire, Madame la Conseillère fédérale, à l'assurance de sa haute considération.

Au nom du Conseil d'Etat

Le président

Frédéric Favre

Le chancelier

Philipp Spörri

Kanton Zürich
Regierungsrat

Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

22. September 2021 (RRB Nr. 1044/2021)

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (Vernehmlassung)

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 23. Juni 2021 haben Sie uns den Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) zur Vernehmlassung unterbreitet. Wir danken für die Gelegenheit zur Stellungnahme und äussern uns wie folgt:

1. Vorbemerkungen

Kantone und Gemeinden sind von der Datenschutzverordnung des Bundes zwar nicht unmittelbar betroffen. Der Verordnungsentwurf kann ihnen jedoch als Orientierungshilfe dienen, um das kantonale bzw. kommunale Recht an die raschen technologischen und rechtlichen Entwicklungen anzupassen, die im Zusammenhang mit der Bearbeitung von Personendaten auf europäischer und auf eidgenössischer Ebene zu beobachten sind. Zudem diente die Revision des Bundesgesetzes vom 25. September 2020 über den Datenschutz (nDSG) neben der Anpassung des Datenschutzes an die technologische Entwicklung und an die Herausforderungen der Digitalisierung vorab dem Ziel, dass die Schweiz von der EU weiterhin als Drittstaat mit angemessenem Datenschutz anerkannt wird. Ohne einen entsprechenden Angemessenheitsbeschluss der EU und ohne den freien Datenverkehr wären beträchtliche Wettbewerbsnachteile für die Schweiz zu erwarten. Mit dem vorliegenden Verordnungsentwurf sollte dies erreicht werden. Die vorliegenden Ausführungsbestimmungen erhöhen jedoch den Umsetzungsaufwand für Unternehmen. Soweit der Angemessenheitsbeschluss der EU nicht gefährdet wird, ersuchen wir Sie, deshalb zu prüfen, ob Anforderungen, die zu einem erheblichen administrativen Aufwand für Unternehmen führen, in Teilbereichen begrenzt werden können (vgl. auch die nachfolgenden Bemerkungen zu einzelnen Bestimmungen).

2. Zu den Bestimmungen im Einzelnen

Vorbemerkungen zu Art. 1–4 E-VDSG (Datensicherheit):

Art. 1–4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit gemäss Art. 8 nDSG. Unseres Erachtens fehlen den Bestimmungen objektive Tatbestandsmerkmale bezüglich der strafbaren Unterlassung (Art. 61 Abs. 1 Bst. c nDSG). Für die Rechtsunterworfenen ist damit nicht klar, wann sie sich strafbar machen. Mit Bezug auf die Datensicherheit weisen wir zudem darauf hin, dass mit dem Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit (Informationssicherheitsgesetz) ebenfalls Anforderungen an die Datensicherheit formuliert wurden. Auch wenn der Geltungsbereich der Gesetze nicht deckungsgleich ist, sollten die Grundsätze doch übereinstimmen. Wir regen deshalb an, die Bestimmungen mit Blick auf das Informationssicherheitsgesetz zu überarbeiten. Die Regelung müsste Kriterien zur Beurteilung des Schutzbedarfs und der Risiken enthalten und entsprechende Sicherheitsmassnahmen vorschlagen.

Zu Art. 1 E-VDSG:

Zu Abs. 1: Es sollte entsprechend Art. 32 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO) vom 27. April 2016 in den Vordergrund gestellt werden, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Dazu sind die Schutzziele, die in Art. 5 Bst. h nDSG aufgezählt sind, der Schutzbedarf (Art. 1 Abs. 1 Bst. a E-VDSG) und die Risiken (entsprechend Art. 22 nDSG) zu ermitteln und gestützt darauf die angemessenen Massnahmen festzulegen. Diese Grundsätze sollten aus der Bestimmung klarer hervorgehen.

Zu Art. 2 E-VDSG:

Die Aufzählung der Schutzziele wurde aus der geltenden Verordnung übernommen und mit Bestimmungen aus der DSGVO ergänzt. Im Grundsatz gehen die Schutzziele bereits aus Art. 5 Bst. h nDSG hervor und lassen sich mit den folgenden, in der Informatiksicherheit üblichen Schutzzielen zusammenfassen: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit (so auch Erläuternder Bericht, S. 15). Wir regen an, die Schutzziele in einer verständlicheren Weise umzuformulieren.
Zu ergänzen ist, dass der Einleitungssatz missverständlich ist: Die Massnahmen müssen angemessen sein in Bezug auf die in der Risikobeurteilung festgestellten Risiken und nicht in Bezug auf die Schutzziele.

Zu Art. 3 E-VDSG:

Art. 3 E-VDSG sieht eine ausführliche Protokollierung der Datenbearbeitungen sowohl für private Verantwortliche als auch für die Bundesorgane vor. Unseres Erachtens wird mit der vorgeschlagenen Regelung die Protokollierung als Massnahme der Informatiksicherheit überbewertet. Die Protokollierung hat zum Zweck, dass in Situationen, in denen ein unberechtigtes Bearbeiten von Personendaten nicht von vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und unter Umständen sanktioniert) werden kann. Sie ergibt sich folglich aus der Risikobeurteilung und der Massnahmenplanung und soll insbesondere angeordnet werden, wenn besonders schützenswerte Personendaten bearbeitet werden. Dies ist im Rahmen der Abklärungen gemäss einem angepassten Art. 1 zu ermitteln, weshalb wir die Weglassung von Art. 3 E-VDSG anregen.

Die Vorgabe für die privaten Verantwortlichen, bei bestehenden hohen Risiken eine Protokollierung umzusetzen (Art. 3 Abs. 1 E-VDSG), widerspricht zudem dem Konzept, keine konkreten Massnahmen festzulegen (Erläuternder Bericht, S. 14), und verkennt in dieser absoluten Form die Möglichkeiten der Protokollierung.
Sodann sollen die Protokolle gemäss Art. 3 Abs. 4 E-VDSG während zwei Jahren aufbewahrt werden und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei ist in Betracht zu ziehen, dass diese Vorgabe zum Aufbau riesiger Datensammlungen führen würde, was Missbrauchspotenzial mit sich bringen würde. Je nach Ziel der Protokollierung (Überwachung der Datenschutzvorschriften, Wiederherstellung von Sicherheitslücken) ist eine Aufbewahrung von wenigen Tagen oder Monaten angemessen.

Zu Art. 4 E-VDSG:

Die Erstellung eines Bearbeitungsreglements wird für private Verantwortliche und deren Auftragsbearbeitende beschränkt auf die Fälle, in denen diese «umfangreich besonders schützenswerte Personendaten bearbeiten» (Abs. 1 Bst. a) oder «ein Profiling mit hohem Risiko durchführen» (Abs. 1 Bst. b). Durch diese Beschränkung wird nur ein Teil der für die Persönlichkeitsrechte kritischen Datenbearbeitungen abgedeckt. Ein Reglement sollte dann nötig sein, wenn die Voraussetzungen zur Vornahme einer Datenschutz-Folgenabschätzung gegeben sind (Die Bearbeitung weist ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen auf, Art. 22 Abs. 1 nDSG). Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 nDSG), die Teil des Bearbeitungsreglements sein können.
Art. 4 Abs. 2 E-VDSG enthält Mindestanforderungen für das Datenbearbeitungsreglement. Es sollte hier ein Konnex zu den Standards in der Informatik hergestellt werden: Es könnte auf diese verwiesen und beim Vorhandensein einer Zertifizierung (z. B. ISO 27001) auf die separate Erstellung eines Datenbearbeitungsreglements verzichtet werden.
Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater ist die Fachperson bei einem Verantwortlichen, und ein Bearbeitungsreglement wird zusammen mit ihr oder ihm erstellt und nicht «der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständliche Form zur Verfügung» gestellt. Es gehört zu den Aufgaben der Datenschutzberaterin oder des Datenschutzberaters, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b nDSG). Zudem muss die Datenschutzberaterin oder der Datenschutzberater über die erforderlichen Fachkenntnisse verfügen (Art. 10 Abs. 3 Bst. c nDSG). Art. 4 Abs. 3 E-VDSG ist deshalb wegzulassen.

Zu Art. 5 E-VDSG:

Wir verweisen hierzu auf die Ausführungen zu Art. 4 E-VDSG.

Zu Art. 7 E-VDSG:

Auch die Datenschutzberaterin oder der Datenschutzberater des Bundesorgans hat bei der Anwendung der Datenschutzvorschriften mitzuwirken. Es widerspricht dem präventiven und risikoorientierten Ansatz des nDSG, wenn die Datenschutzberaterin oder der Datenschutzberater lediglich nachträglich über den Abschluss eines Outsourcingvertrages oder

bei einer Funktionsübertragung informiert werden soll. Es ist eine Kernaufgabe einer Datenschutzberaterin oder eines Datenschutzberaters, bei solchen Geschäften mitzuwirken («Mitwirkung bei der Anwendung der Datenschutzvorschriften»). Die Datenschutzberaterin oder der Datenschutzberater ist rechtzeitig zu informieren, wie dies bei den Datenbearbeitungsprojekten vorgesehen ist (Art. 31 E-VDSG). Art. 7 E-VDSG ist deshalb wegzulassen.

Art. 8 E-VDSG:

Bei den Formulierungen in Art. 8 E-VDSG fällt auf, dass die oder der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) konsultiert wird (Abs. 6), während die Beurteilungen von internationalen Organisationen oder ausländischen Behörden berücksichtigt werden können (Abs. 2). Mit einer Anpassung der Formulierung ist klarzustellen, dass auch die Stellungnahmen des EDÖB berücksichtigen werden können.

Zu Art. 13 E-VDSG:

Art. 19 nDSG enthält keine direkte Informationspflicht der Auftragsdatenbearbeiterin oder des Auftragsdatenbearbeiters. Eine Informationspflicht der Auftragsdatenbearbeiterin oder des Auftragsdatenbearbeiters kann sich deshalb nur aus einem Auftrag ergeben. In der Verordnung kann sie unseres Erachtens nicht geschaffen werden.

Zu Art. 18 E-VDSG:

Art. 18 E-VDSG schreibt vor, dass eine Datenschutz-Folgenabschätzung schriftlich festzuhalten und bis zwei Jahre nach Beendigung der Datenbearbeitung aufzubewahren ist. Wir bezweifeln den Nutzen dieser Aufbewahrungspflicht. Einerseits fliessen die Ergebnisse der Datenschutz-Folgenabschätzung direkt in die beurteilte Datenbearbeitung ein und anderseits ist die Datenschutz-Folgenabschätzung als Momentaufnahme sehr schnell veraltet. Es erscheint als ausreichend, die Datenschutz-Folgenabschätzung nach Aufnahme der Datenbearbeitung noch ein Jahr aufzubewahren.

Zu Art. 19 E-VDSG:

Art. 24 Abs. 1 nDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 nDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 nDSG).
Mit Art. 24 nDSG wird (bewusst) von Art. 33 DSGVO abgewichen. Dennoch werden in Art. 19 E-VDSG die Bestimmungen von Art. 33 DSGVO weitgehend übernommen. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen, was für die Mehrheit der Verantwortlichen nicht der Fall ist. Art. 19 E-VDSG bringt damit unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde und allenfalls auch die betroffenen Personen rasch informiert werden und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden. Eine Konkretisierung von Art. 24 nDSG durch Art. 19 E-VDSG erscheint nicht nötig.

Zudem ist die in Art. 19 Abs. 5 E-VDSG vorgesehene Aufbewahrungsdauer der Unterlagen von drei Jahren nicht nachvollziehbar, weil die Unterlagen in einem Strafverfahren nur mit der Einwilligung der meldepflichtigen Person verwendet werden dürfen. Es ist ausreichend, wenn die Aufsichtsbehörde die Meldung nach den für sie ohnehin geltenden Aufbewahrungsvorschriften aufbewahrt. Eine Spezialbestimmung ist nicht erforderlich.

Zu Art. 20 E-VDSG:

Art. 25 f. nDSG regeln das Auskunftsrecht und dessen Einschränkungen ausführlich. Art. 20 E-VDSG bringt hierzu zwar einige Konkretisierungen, diese sind jedoch nur zum Teil notwendig.
Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 nDSG festgelegt. Daraus ergeben sich der Umfang und der Zweck der Auskunft. Dies bemisst sich nach objektiven Kriterien. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für die Verantwortlichen bedeuten, dass sie mehr Angaben zu dieser Person bearbeiten müssten und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse der Verantwortlichen integriert werden könnte. Art. 20 Abs. 3 E-VDSG ist deshalb wegzulassen.
Art. 20 Abs. 4 E-VDSG verpflichtet die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen». Dies ergibt sich bereits aus Art. 8 nDSG und den Bestimmungen des 1. Kapitels der E-VDSG, weshalb dieser Hinweis in Art. 20 Abs. 4 E-VDSG wegzulassen ist.
Art. 26 Abs. 4 nDSG sieht vor, dass die oder der Verantwortliche angeben muss, weshalb die Auskunft verweigert, eingeschränkt oder aufgeschoben wird. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an die Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne ersichtliche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person. Art. 20 Abs. 5 E-VDSG ist deshalb wegzulassen.

Zu Art. 21 E-VDSG:

Art. 21 Abs. 1 E-VDSG sieht vor, dass Verantwortliche, die für die Behandlung eines Begehrens nicht zuständig sind, dieses dem zuständigen Verantwortlichen weiterleiten. Dies kann im öffentlich-rechtlichen Bereich vorgesehen werden. Im privatrechtlichen Verhältnis legen die Parteien ihre Rechte und Pflichten aber autonom fest. Die gleiche Auflage auch dem privatrechtlichen Verantwortlichen zu machen, ist deshalb unverhältnismässig. Sie führt zu einem Aufwand für die privatrechtlichen Verantwortlichen, die «zuständigen» Verantwortlichen ausfindig zu machen, ohne dass dadurch die Rechte der betroffenen Personen gestärkt würden. Art. 21 Abs. 1 zweiter Satz E-VDSG ist deshalb anzupassen.

Zu Art. 24 E-VDSG:

Art. 24 E-VDSG enthält eine Konkretisierung von Art. 28 nDSG, indem auf die sinngemässe Anwendung von Bestimmungen zum Auskunftsrecht verwiesen wird. Dies wird dem neuen Rechtsinstitut der «Datenportabilität» nicht gerecht und verkennt den durchaus vorhandenen Bedarf einer Konkretisierung der gesetzlichen Bestimmung (beispielsweise in

Bezug auf die «gängigen elektronischen Formate» oder den «unverhältnismässigen Aufwand» bei der direkten Übertragung von einem Verantwortlichen zu einem anderen). Zudem wäre auch in Bezug auf die Ausnahmen der Kostenlosigkeit eine andere Regelung als beim Auskunftsrecht denkbar, da hier nicht der Persönlichkeitsschutz, sondern der wirtschaftliche Wert der Daten im Vordergrund steht. Wir regen deshalb eine Überprüfung der Bestimmung an.

Zu Art. 25 E-VDSG:

Art. 25 E-VDSG hält fest, welche Aufgaben die Datenschutzberaterin oder der Datenschutzberater wahrnehmen muss. Es wird dabei kein Bezug auf Art. 10 Abs. 2 nDSG genommen, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die sie oder er wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 nDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist deshalb missverständlich und sollte angepasst werden.

Zu Art. 26 E-VDSG:

In Anwendung von Art. 12 Abs. 5 nDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn «umfangreich besonders schützenswerte Personendaten bearbeitet» werden (Bst. a) oder «ein Profiling mit hohem Risiko durchgeführt» wird (Bst. b). Wir verweisen auf unsere Ausführungen zu Art. 4 Abs. 1 E-VDSG und erachten es auch hier als angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Die Bearbeitung weist ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen auf; Art. 22 Abs. 1 nDSG).

Zu Art. 36 E-VDSG:

Diese Bestimmung ist nicht nötig. Die angestrebte Präzisierung (Bearbeitung nur für nicht personenbezogene Zwecke) ergibt sich bereits aus dem Ingress von Art. 39 nDSG ausreichend klar.

Genehmigen Sie, sehr geehrte Frau Bundesrätin,
die Versicherung unserer ausgezeichneten Hochachtung.

Im Namen des Regierungsrates

Die Präsidentin: Jacqueline Fehr

Die Staatsschreiberin: Dr. Kathrin Arioli

Allianza dal Center | Alleanza del Centro | Le Centre | Die Mitte

Per Mail: jonas.amstutz@bj.admin.ch

Bern, 11. Oktober 2021

Vernehmlassung: Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

Sie haben uns eingeladen, zur oben genannten Vernehmlassungsvorlage Stellung zu nehmen. Für diese Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens.

Allgemeine Bemerkungen
Die Mitte begrüsst prinzipiell das revidierte Bundesgesetz über den Datenschutz und die Verordnung zum Bundesgesetz über den Datenschutz. Denn wir wollen ein modernes Datenschutzrecht mit hohen Standards beim Konsumentenschutz und bei der Sicherheit der Privatsphäre. Dieses Datenschutzrecht muss jedoch zweckmässig sein, es muss administrativ auch für KMU und Startups umsetzbar sein und darf die Innovationskraft des Wirtschaftsstandorts Schweiz nicht bremsen. Denn wir wollen das Potential der digitalen Transformation ausschöpfen. Der Aufwand und die damit erreichte Erhöhung des Datenschutzes müssen daher in einem angemessenen Verhältnis stehen. Auch sind sogenannte «Swiss Finishes», das heisst Regulierungen, die über den notwendigen Anpassungsbedarf hinausgehen, zu vermeiden.

Swiss Finishes und internationaler Kontext
Datenschutz darf nicht an unseren Grenzen enden. Wir unterstützen daher, dass die Vorgaben der Verordnung klar in einem internationalen Kontext eingebettet sind. So spricht sich die Mitte explizit dafür aus, dass die Verordnung mit der europäischen Datenschutz-Grundverordnung kompatibel ist. Damit eine grenzüberschreitende Datenübermittlung zwischen der Schweiz und den EU-Staaten beidseitig ohne zusätzliche Hürden möglich bleibt, müssen jedoch jegliche «Swiss Finishes», die über den notwendigen Anpassungsbedarf gehen, vermieden werden: das DSG, beziehungsweise die VDSG dürfen daher nicht strenger sein als die DSGVO. Leider ist dies entgegen den Entscheidungen des Parlaments in der Verordnung zum Teil der Fall. Die Mitte bittet darum, dass dies korrigiert wird, beispielsweise in Art. 13 Abs. 1 bezüglich der Modalitäten der Informationspflichten, welche sich gemäss Gesetz und DSGVO nur auf den Verantwortlichen beziehen und nicht auf den Auftragsbearbeiter.

Das Auskunftsrecht in Art. 20 ist ein essenzieller Teil einer effektiven Datenschutzregelung. Wir begrüssen daher die Konkretisierung des Auskunftsrechts, welches dazu verpflichtet, Auskunftsbegehren binnen einer spezifischen Frist zu beantworten. Die Aufbewahrungspflicht aus Art. 20 Abs. 5 kennt jedoch keine Grundlage in der DSGVO. Zudem sollte die maximale Beteiligung an den Kosten bei Art. 23 Abs. 2 erhöht werden, beziehungsweise an den effektiven Aufwand gekoppelt werden, da die Auskunftserteilung mit einem Aufwand von über 300 Franken verbunden sein kann.

Beim Auskunftsrecht sollte zudem Art. 21 Abs. 1 Satz 2 gestrichen werden, da in der Praxis ein Verantwortlicher nicht immer klarstellen kann, ob und welche weiteren Verantwortlichen ebenfalls zuständig sein könnten. Auch sollte Art. 21 Abs. 2 präzisiert werden, da anhand der jetzigen Formulierung ein Verantwortlicher, eine mögliche Verantwortung nach eigenem Ermessen von sich weisen könnte, um sie unbegründeterweise an einen Auftragsbearbeiter weiterzuleiten.

Die Mitte Hirschengraben 9, Postfach, CH-3001 Bern
T 031 357 33 33, F 031 352 24 30, info@die-mitte.ch, www.die-mitte.ch, PC 30-3666-4

In Art. 8 begrüssen wir die Konkretisierung der Beurteilungspflicht über die Gewährleistung von Datenschutzstandards, wenn Personendaten ins Ausland geleitet werden, insbesondere zur Achtung der Menschenrechte. Allerdings kann nur der Bundesrat eine verbindliche Positivliste erstellen. Dies sollte, der Klarheit halber, in Art. 8 präzisiert werden.

Die Ausführungsverordnung bedarf Grundlagen im Gesetz
Jeder Punkt der Verordnung bedarf einer Grundlage im Gesetz. Mehrere Regelungen in der Verordnung gehen unseres Erachtens jedoch über diesen Rahmen hinaus. So geht beispielsweise die Protokollierungs- und Aufbewahrungspflicht in Art. 3 über das Gesetz hinaus und würde gerade für KMU einen beträchtlichen Aufwand generieren. Auch Art. 15 entwickelt bei der Bekanntgabe von Personendaten Anforderungen, welche keine Grundlage im Gesetz kennen und starke Zusatzanforderungen bedeuten würden. Dasselbe gilt für Art. 16 bezüglich der Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten. Diese Punkte, die vom Parlament abgelehnt wurden, dürfen nun nicht über die Verordnung wieder eingeführt werden.

Praktikables Datenschutzrecht
Wir setzen uns für ein Datenschutzrecht ein, welches für die gesamte Schweizer Wirtschaft praktikabel ist, vom international tätigen Grossunternehmen bis zum KMU oder Startup. Wir unterstützen daher die Ausnahmen in Art. 26 der Verordnung von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten für Unternehmen, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen. Allerdings sollte präzisiert werden, dass die Pflicht zur Führung eines Verzeichnisses im Falle der Bearbeitung von besonders schützenswerte Personendaten sich auf die Vorgänge mit besonders schützenswerten Personendaten beschränkt und nicht auf alle Vorgänge des Unternehmens bezieht.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und verbleiben mit freundlichen Grüssen.

Die Mitte

Sig. Gerhard Pfister
Präsident Die Mitte Schweiz

Sig. Gianna Luzio
Generalsekretärin Die Mitte Schweiz

FDP
Die Liberalen

FDP.Die Liberalen
Generalsekretariat
Neuengasse 20
Postfach
CH-3001 Bern

+41 (0)31 320 35 35
www.fdp.ch
info@fdp.ch
/fdp.dieliberalen
@FDP_Liberalen

FDP.Die Liberalen, Postfach, 3001 Bern

Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

Elektronischer Versand:
jonas.amstutz@bj.admin.ch

Bern, 8. Oktober 2021
VDSG/ DD

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)/ Vernehmlassungsantwort der FDP.Die Liberalen

Sehr geehrte Damen und Herren

Für Ihre Einladung zur Vernehmlassung oben genannter Vorlage danken wir Ihnen. Gerne geben wir Ihnen im Folgenden von unserer Position Kenntnis.

FDP.Die Liberalen lehnt den in Vernehmlassung gegebenen Entwurf der Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) ab und beantragt dessen Überarbeitung.

Ein solider Datenschutz ist ein grundliberales Anliegen. Eine zeitgemässe, praktisch umsetzbare und international abgestimmte Datenschutzgesetzgebung ist zudem von hoher wirtschaftlicher Bedeutung. Die FDP hatte sich deshalb im Parlament bei der Totalrevision des Datenschutzgesetzes für ein Datenschutzgesetz stark gemacht, das eben diesen Anforderungen entspricht. Dabei legte sie besonderen Wert darauf, dass den rechtlichen Entwicklungen auf europäischer Ebene Rechnung getragen und auf für Schweizer Unternehmen schädliche «Swiss finishes» verzichtet wurde. Diese komplexe Aufgabe konnte das Parlament nach langen Beratungen mit der Verabschiedung des revidierten Datenschutzgesetzes (revDSG) schlussendlich erfolgreich abschliessen. Es wurde ein austarierter Kompromiss gefunden, den die FDP mittrug.

Der E-VDSG trägt nun aber diesen parlamentarischen Beratungen des revDSG und der Zielsetzung des Revisionsvorhabens nicht genügend Rechnung: Der praktischen Umsetzbarkeit wurde beispielsweise bei der Revision des DSG ein hoher Stellenwert beigemessen. Von Unternehmen sollte nur verlangt werden, was sie auch realistischerweise erfüllen können. Der E-VDSG jedoch wirkt diesem Ziel entgegen. So sind die vorgeschlagenen Vorschriften zur Datensicherheit (Art. 2 E-VDSG) nicht, wie in Art. 8 Abs. 3 revDSG verlangt, als Mindestanforderungen ausgestaltet. Vielmehr stellen sie breit gefächerte, ambitionierte Schutzziele dar, deren Erfüllung angesichts der heutigen Cyberrisiken kaum realistisch ist. Verschlimmert wird dieser Umstand dadurch, dass die Verletzung der Mindestanforderungen gem. Art. 60 revDSG mit Strafe bedroht ist. Weiter wird das E-VDSG einem zweiten Grundziel der Revision des DSG, der internationalen Abstimmung, nicht gerecht. Konnten «Swiss finishes» im revDSG noch auf ein Minimum reduziert werden, so erschafft der E-VDSG ohne Not neue Abweichungen (z.B. Art. 4 Abs. 1 und Art. 13 Abs. 1 E-VDSG). Diese führen für unsere Schweizer Unternehmen mehrfachen Datenschutzstandards, die es zu beachten gilt, und damit zu einem mehrfachen Aufwand. Gerade für KMU wird dies zu einem kaum tragbaren Wettbewerbsnachteil führen.

Weiter leidet der E-VDSG an rechtsstaatlichen Mängeln, indem er die Regelungskompetenz der Exekutive überschreitet. Beim E-VDSG handelt es sich um die Ausführungsverordnung zum revDSG. Sein Inhalt entspricht aber in zahlreichen Punkten nicht einer Ausführungsverordnung: Der E-VDSG statuiert neue Pflichten, für die das revDSG keine gesetzliche Grundlage bietet (Art. 13 E-DSG). Zudem führt er Regelungen auf, die in ihrer Bedeutung den in der revDSG enthaltenen Bestimmungen gleichkommen und daher entweder auf gesetzlicher Ebene – im revDSG – zu statuieren wären (z.B. Art. 4, Art. 15 und Art. 16) oder einer entsprechenden Delegationsnorm als Grundlage auf Gesetzesstufe bedürfen würden. Der Art. 16 E-VDSG befand sich gar ursprünglich im Entwurf des revDSG, wurde jedoch im Laufe des parlamentarischen Verfahrens gestrichen und widerspricht damit zusätzlich dem expliziten Willen des Gesetzgebers.

In Kombination führen diese Mängel des E-VDSG zu einem nicht unerheblichen Überarbeitungsbedarf, der sinnvollerweise im Rahmen einer gesamthaften Überprüfung angegangen werden sollte.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Überlegungen.

Freundliche Grüsse

FDP.Die Liberalen

Der Präsident	Die Generalsekretärin
Thierry Burkart Ständerat	Fanny Noghero

GRÜNE Schweiz
Waisenhausplatz 21
3011 Bern

rahel.estermann@gruene.ch
031 326 66 15

Eidgenössisches Justiz- und Polizeidepartement, Frau Bundesrätin Karin Keller-Sutter
3003 Bern

per E-Mail an:
jonas.amstutz@bj.admin.ch

Bern, 14. Oktober 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG): Vernehmlassung

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Sie haben die GRÜNEN für eine Stellungnahme zur Verordnung zum Bundesgesetz über den Datenschutz eingeladen. Wir danken Ihnen für die Gelegenheit, uns zur Vorlage zu äussern.

Mit dem neuen Datenschutzgesetz (nDSG) und der Totalrevision der Verordnung zum Datenschutzgesetz (VDSG) erfolgt eine Annäherung an die europäische Datenschutzgrundverordnung (DSGVO), die global zu einem wichtigen Orientierungspunkt für den rechtlichen Schutz der Privatsphäre geworden ist. Die GRÜNEN begrüssen es, dass auch die Schweiz wichtige Schritte in diese Richtung unternimmt.

Personen, Organisationen und Unternehmen müssen aufgrund dieser Entwicklungen ihre Prozesse datenschutztechnisch überprüfen und verbessern. Die VDSG soll ihnen dabei als rechtliche Vorgabe dienen. Allerdings ist uns aufgefallen, dass viele Begriffe in der VDSG schwammig bleiben – uns erscheint es deshalb fragwürdig, ob die VDSG eine genügende Anleitung für die Verantwortlichen schafft, die für eine angemessene Umsetzung der Regulierungen zuständig sind.

Zu den Artikeln nehmen wir im Detail wie folgt Stellung:

Kapitel 1, Abschnitt 1 (Datensicherheit)
Art. 1 Abs. 1, Bst. D erwähnt als die “Implementierungskosten” als eines mehrerer Kriterien zur Beurteilung von Massnahmen zur Gewährleistung der Datensicherheit. Es irritiert uns GRÜNE, dass die Kosten ein Kriterium sind: Es soll nicht von den Kosten abhängen, ob eine Massnahme angemessen ist, den Datensicherheits-Risiken zu begegnen. Zwar sagen die

Erläuterungen (S. 16), dass die Kosten keine Ausrede sein dürfen; und dass dieses Kriterium nur dann zum Zug kommt, wenn verschiedene (gleich) wirksame Massnahmen zur Auswahl stehen. Dies wird aber in den Bestimmungen nicht so abgebildet, sondern das Kriterium erscheint gleichwertig wie die Kriterien in den Bestimmungen a, b und c. **Wir erwarten deshalb eine Überarbeitung dieses Absatzes im Sinne dieser Ausführungen.**

Art. 2 gibt die Schutzziele der Datensicherheit vor. Allerdings werden diese verwässert, indem diese lediglich «soweit angemessen» zu erreichen sind. Dies eröffnet für die Verantwortlichen Ermessensspielräume, welche der Datensicherheit zuwiderlaufen können. **Wir beantragen deshalb, die Formulierung «soweit angemessen» zu streichen.**

Die von Art. 3 vorgegebene Protokollierungspflicht begrüssen wir sehr, sie ist wichtig für die Datensicherheit. Der Art. 4, welche die Massnahmen für Verantwortliche regelt, die besonders schützenswerte Personendaten bearbeiten oder ein Profiling mit hohem Risiko durchführen, ist aus unserer Sicht ein Kernstück des künftigen Datenschutzes in der Schweiz.

In Art. 4 Abs. 1 ist die Erstellung eines Bearbeitungsreglements für private Verantwortliche und deren Auftragsbearbeiter vorgesehen, die (1) umfangreich besonders schützenswerte Personendaten bearbeiten oder (2) ein Profiling mit hohem Risiko durchführen. Diese Eingrenzung erscheint willkürlich und deckt bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen ab. **Hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen**: Wenn die Bearbeitung ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen beinhaltet, siehe Art. 22 Abs. 1 nDSG).

Wir möchten noch eine grundsätzliche Forderung zum 1. Abschnitt (Art. 1 bis 5) einbringen. Diese Artikel zur Datensicherheit erlauben es leider nicht, zu beurteilen, ob die «Mindestanforderungen» gemäss nDSG Art. 8 Abs 3 von den Verantwortlichen erfüllt bzw. die notwendigen Bemühungen unterlassen wurden. Dies ist ein weiteres Beispiel für die bereits erwähnte Tendenz, dass die VDSG nicht genügend Klarheit und präzise Leitlinien schafft. Dabei gäbe es Konzepte – beispielsweise im ISG, Art. 17 –, welche den Schutzbedarf bei Daten sowie die Risiken in Kategorien einteilen und daraus klare Vorgaben für die nötigen Massnahmen ableiten. Dies fehlt im VDSG. **Wir GRÜNE schlagen deshalb vor, den Abschnitt 1 der VDSG in diesem Sinne zu überarbeiten.**

<u>Kapitel 1, Abschnitt 3 (Bekanntgabe von Personendaten ins Ausland)</u>

In Art. 8 (Angemessenheitsbeurteilung) erscheint uns mehr Transparenz nötig, dieser Grundsatz wurde in diesem Artikel nicht umgesetzt. Der bisher verantwortliche EDÖB hat regelmässig auf seiner Webseite über aktuelle Entwicklungen und Anpassungen informiert. Auch der Bundesrat ist nun gehalten, seine Entscheidungen transparent der Öffentlichkeit zugänglich zu machen. **Wir beantragen deshalb, Art. 8 Abs. 3 zu ergänzen mit dem Satz: «Entscheidungen, Änderungen und Anpassungen sind der Öffentlichkeit begründet, unverzüglich und vollständig zugänglich zu machen».**

Die VDSG soll zudem Art. 8 Abs. 5 insofern präzisieren, dass der EDÖB nicht nur konsultiert wird, sondern seine Stellungnahmen auch materiell in der Beurteilung zu berücksichtigen sind.

Kapitel 2

In Art. 13 Abs. 1, der sich eigentlich an der DSGVO (Art. 12) orientiert, fällt auf: Das Adjektiv «transparent» fehlt in der Aufzählung («präziser, verständlicher und leicht zugänglicher Form»). **Wir gehen von einem Versehen aus und erwarten eine Korrektur bzw. Ergänzung des Wortes.**

Kapitel 3, Abschnitt 1 (Auskunftsrecht)

Es befremdet uns GRÜNE, dass Art. 20 Abs. 1 vorsieht, dass die Form der Auskunft vom Willen der Verantwortlichen abhängig gemacht wird («Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden»). Das Auskunftsrecht ist ein zentraler Grundsatz des Datenschutzes und soll so wenig als möglich eingeschränkt werden. **Die Verordnung muss deshalb das schriftliche oder mündliche Begehren gleichwertig festschreiben oder auf eine Formvorgabe verzichten.**

In Art. 22, welcher die Fristen für die Auskunft regelt, relativiert leider Abs. 2 den vorangehenden wichtigen Abs. 1, welcher 30 Tage festschreibt. **Abs. 2 muss mit einer Maximalfrist ergänzt werden, damit nicht eine Aufschubsklausel entsteht, welche es ermöglicht, die Auskunftsfrist auf unbestimmte Zeit zu verlängern.**

Art. 23 legt Ausnahmen von der kostenlosen Auskunft fest. Aus unserer Sicht darf das nicht durch die Abschreckungswirkung von Kosten ausgehöhlt werden. Dabei ist es aber wichtig: Gemäss dem Grundsatz «Privacy by Design» sind die Verantwortlichen verpflichtet, ein System zu führen, das einen einfachen Zugang zu den bearbeiteten Daten ermöglicht (auch die Erläuterungen zur VDSG äussern sich in diesem Sinne). Falls die Verantwortlichen aufgrund eigenen Unvermögens einem «unverhältnismässigen» Aufwand aufgrund eines Auskunftsgesuches gegenüberstehen, ist dies in keinerlei Weise Grund zur Auferlegung von Kosten auf betroffene Personen. **Deshalb ist Artikel 23 VDSG dahingehend zu ändern, dass die Auskunftserteilung immer kostenlos ist, unabhängig des Aufwands und im seltenen Falle eines klar rechtsmissbräuchlichen Auskunftsbegehrens, dieses abgewiesen würde.** Verantwortliche, die häufig oder komplex Auskunft erteilen müssen, erhalten so auch einen Anreiz, die Auskunftserteilung zu automatisieren.

Kapitel 3, Abschnitt 2 (Recht auf Datenherausgabe oder -übertragung)

Die Datenherausgabe und -portabilität ist eine zentrale Errungenschaft in einer digitalen Welt, die leider zunehmend in Datensilos organisiert ist, deren Wände undurchdringlich gemacht werden. Art. 24 wird dieser Errungenschaft leider nicht gerecht; er gibt einfach vor, die Bestimmungen zu Auskunftsrecht sollen sinngemäss auch für die Datenportabilität umgesetzt werden. Dabei wären gerade für eine leistungsfähige Datenportabilität präzise Vorgaben über das Format nötig. So ist es irritierend, dass nDSG Art. 28 ein elektronisches Format vorgibt, während die Verordnung im Auskunftsrecht (Art. 20) nur von «schriftlich» spricht. Die Verordnung wird der Intention der Datenherausgabe und -portabilität somit nicht gerecht und hinterlässt bezüglich Format grosse Unklarheiten. **Art. 24 muss aus Sicht der GRÜNEN entsprechend überarbeitet werden.**

Kapitel 4 (Besondere Bestimmungen)

Art. 26 nennt Organisationen, die kein Datenbearbeitungs-Verzeichnis führen müssen. Der Artikel setzt nDSG Art. 12 Abs. 5 um, welcher Unternehmen mit weniger als 250 Mitarbeitenden und geringen Risiken von dieser Pflicht ausnimmt. Ein hohes Risiko wird gemäss Art. 26 im Entwurf daran festgemacht, dass «umfangreich besonders schützenswerte Personendaten bearbeitet» werden oder «ein Profiling mit hohem Risiko durchgeführt» wird. Aus Sicht

der GRÜNEN sind durch diese Kriterien nicht alle für die Persönlichkeitsrechte kritischen Datenbearbeitungen abgedeckt. **Wir schlagen vor, hier die Voraussetzungen für die Datenschutz-Folgeabschätzung zu übernehmen: die Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen, siehe nDSG Art. 22 Abs. 1).**

Wir danken Ihnen, Frau Bundesrätin, sehr geehrte Damen und Herren, für die Überarbeitung des Entwurfs gemäss unseren Vorschlägen.

Freundliche Grüsse

Balthasar Glättli
Präsident

Rahel Estermann
stv. Generalsekretärin, Leiterin Politik

piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Sehr geehrter Frau Bundesrätin
Sehr geehrte Damen und Herren

Stellungnahme zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) (Vernehmlassung 2021/26)

Bezugnehmend auf Ihre Vernehmlassungseröffnung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 23.06.2020 nehmen wir gerne Stellung und würden es zukünftig sehr begrüssen, wenn wir in Ihre Adressatenliste aufgenommen werden.

Im Weiteren finden wir Piraten es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen Ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

Vorbemerkungen

Neben unseren Ausarbeitungen zur Vernehmlassung an der Verordnung zum Bundesgesetz über den Datenschutz möchten wir noch kurz Anmerkungen zum zu Grunde liegenden Gesetz anfügen.

Die Etablierung der Definition "Profiling mit hohem Risiko" erachten wir als sehr bedenklich. Jegliches Profiling hat ein hohes Risiko, eine Unterscheidung ergibt keinen Sinn. Datensparsamkeit ist deshalb grundsätzlich geboten.

Mit dem Urteil "Schrems II" des EuGH sind Standardvertragsklauseln nicht mehr gültig. Der EDÖB hält hierzu explizit fest: "Die zusätzlichen technischen und organisatorischen Massnahmen müssen dergestalt sein, dass die Behördenzugriffe auf die übermittelten Personendaten im Zielland faktisch verhindert werden." [1] Infolge dessen besteht eine Dringlichkeit das DSG anzupassen.

Ferner wird im Artikel 16 nDSG die Angemessensbeurteilung ausländischer Datenschutzgesetzgebung vom EDÖB an den Bundesrat übertragen. Wir befürchten, dass somit

Entscheide politischer Natur und nicht basierend auf Expertise gefällt wird. Um dies zu verhindern muss der EDÖB auch in Zukunft die Beurteilung vornehmen und der Bundesrat dies übernehmen.

Stellungnahme zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

In Art. 2 wäre es wünschenswert, wenn eine klarere Unterscheidung zwischen Unternehmen, bei denen Datenverarbeitung nur administrativer Natur ist, und Unternehmen, deren Geschäftsmodell auf Datenerhebung, Analyse, Bereitstellung und/oder Nutzung basiert, eingeführt würde. Zwar kann argumentiert werden, dass die Klausel "soweit angemessen" diesem Umstand bereits Rechnung trägt, aber letztere Unternehmen sollten diesen Ermessensspielraum weiter eingegrenzt wissen, da ansonsten ein Missbrauch leichter möglich bleibt.

In Art. 6 Abs. 1 vermissen wir die Definition, *wie* die vertrags- oder gesetzesgemässe Bearbeitung mindestens sichergestellt werden muss. So ist es zwar nur recht, dass der Auftraggeber weiterhin die Verantwortung tragen muss. Aber ohne Mindestvorgaben zur Sicherstellung bleibt die korrekte Wahrnehmung dieser Pflicht nicht nur für den Verantwortlichen, sondern auch für die betroffenen Personen unsicher.

Art. 6 Abs. 2 ist wie das nDSG durch das Urteil Schrems II des EuGH[1] bereits wieder veraltet und nicht mehr mit EU-Recht kompatibel. Das kann den Zugang zum digitalen Binnenmarkt der EU gefährden. Um die zukünftige Relevanz der VDSG sicherzustellen, sollte der 2. Satz ("Andernfalls muss er diesen auf vertraglichem Wege sicherstellen") ersatzlos gestrichen oder durch einen Verweis auf EDÖB Richtlinien ersetzt werden, da Standardvertragsklauseln allein nicht mehr ausreichen. Der EDÖB schreibt hierzu:

"Die zusätzlichen technischen und organisatorischen Massnahmen müssen dergestalt sein, dass die Behördenzugriffe auf die übermittelten Personendaten im Zielland faktisch verhindert werden." [2]

Art. 8 Abs. 3-5 behandeln die "Angemessenheit des Datenschutzes" ausländischer Staaten. Darin wird eine periodische Neubeurteilung festgelegt, dessen Ergebnis in Anhang 1 aufgeführt werden soll. Es wäre wünschenswert, nicht nur die Ergebnisse, sondern auch die Entscheidungsfindung transparent zu führen.

Mit der Degradierung des EDÖB zur Konsultationsstelle und der finalen Entscheidungsmacht beim Bundesrat (Art. 16 Abs. 1 DSG i.V.m. Abs. 6 E-VDSG) könnten gewisse Entscheide politischer ausfallen, als es der Sache angemessen wäre. Ein öffentlich und leicht einsehbarer Entscheidungsfindungsprozess würde diesem Problem entgegenwirken.

Art. 23 sieht Ausnahmen von der Kostenlosigkeit für das Auskunftsrecht vor, falls die Auskunft mit einem unverhältnismässigen Aufwand verbunden ist. In Bezug auf Unternehmen sollte auch hier deutlicher zwischen Unternehmen, bei denen Datenverarbeitung nur administrativer Natur ist, und Unternehmen, deren Geschäftsmodell auf Datenerhebung, Analyse, Bereitstellung und/oder Nutzung basiert, unterschieden werden. Der erläuternde Bericht zur Verordnung hat eine solche Unterscheidung bereits angedacht [3], findet sich aber nicht in der Verordnung selbst wieder. Wenn letztere Unternehmen intern effizient mit Daten umgehen können, sollen sie auch sicherstellen müssen, dass sie diese kostenlos aushändigen können. Auskünfte durch den Staat sollten grundsätzlich kostenlos zur Verfügung gestellt werden. Dahingehend muss der Staat auch darauf hinarbeiten seine Daten, Dokumente etc. automatisch der Öffentlichkeit frei zur Verfügung zu stellen.

Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

Quellen:

[1]
https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20DE.pdf.download.pdf/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20DE.pdf [N8]

[2]

https://curia.europa.eu/juris/document/document.jsf;jsessionid=B8741E9212ED1ABD98839AE0EB8F1983?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=10591711

[3] Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, S. 37/87, Art. 23.

———

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 14. Oktober 2021

Bern, 13.10.2021

Per E-Mail

Bundesamt für Justiz

Bundesrain 20

3003 Bern

jonas.amstutz@bj.admin.ch

Vernehmlassungsantwort zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zur Stellungnahme, die wir gerne wir folgt wahrnehmen:

1 Grundsätzliche Bemerkungen

Die SP Schweiz hat in der Vernehmlassung[1] und in den parlamentarischen Debatten[2] zur Totalrevision des Datenschutzgesetzes (nDSG) einen stärkeren Datenschutz für Bürger:innen und Konsument:innen gewünscht als vom Parlament schliesslich beschlossen. Vor diesem Hintergrund ist es für uns zentral, dass der Bundesrat in der Umsetzungsverordnung VDSG den vorhandenen Spielraum konsequent in Richtung von mehr Datenschutz nutzt. Unter diesem Blickwinkel unterstützt die SP Schweiz den Inhalt der vorgeschlagenen Umsetzungsvorlage im Grundsatz, fordert allerdings in einigen Punkten Verbesserungen (siehe dazu nachstehend unter Ziff. 2).

[1] Vgl. Vernehmlassungsantwort SP Schweiz zur Totalrevision des Datenschutzgesetzes, April 2017, Ziff. 1.

[2] Siehe Eintretensvotum NR Cédric Wermuth, NR-Plenumsdebatte 17.059 Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse zum Datenschutz, 24.9.2019.

Sozialdemokratische Partei der Schweiz | Theaterplatz 4 | Postfach · 3001 Bern | Telefon 031 329 69 69 | Telefax 031 329 69 70 | info@spschweiz.ch | www.spschweiz.ch

2 Kommentar zu den wichtigsten Bestimmungen

2.1. Kriterien zur Beurteilung Angemessenheit der Datensicherheitsmassnahmen (Art. 1 Abs. 1 E-VDSG)

Für die SP Schweiz ist es zentral, dass die datenbearbeitenden Personen ausreichende technische und organisatorische Massnahmen zur Gewährleistung der Sicherheit dieser Daten vornehmen. Vor diesem Hintergrund halten wir es für verfehlt, die Implementierungskosten als Beurteilungskriterium zur Angemessenheit solcher Massnahmen explizit in der Verordnung zu erwähnen.[3] So ist für uns z.B. das Risiko einer Verletzung der Datensicherheit das viel relevantere Beurteilungskriterium für die zu treffenden Massnahmen.

Folglich beantragt die SP Schweiz, Art. 1 Abs. 1 E-VDSG folgendermassen zu ändern:

Art. 1 Grundsätze

1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:

a. Zweck, Art, Umfang und Umstände der Datenbearbeitung;

b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen;

c. der Stand der Technik;

~~**d. Implementierungskosten.**~~

2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.

2.2. Schutzziele zur Gewährleistung der Datensicherheit (Art. 2 E-VDSG)

Die SP Schweiz hält es für nicht angebracht, in der Umsetzungsverordnung explizit festzuschreiben, dass die Massnahmen zur Gewährleistung der Datensicherheit die Schutzziele nur insofern erreichen müssten, als diese Massnahmen angemessen seien.[4] Einerseits ist der Angemessenheitsgrundsatz bereits allgemein auf Gesetzesebene verankert (vgl. Art. 6 Abs. 5 nDSG), andrerseits könnte die explizite Erwähnung der

[3] Vgl. Erläuternder Bericht, S. 16.

[4] Siehe Erläuternder Bericht, S. 17.

Angemessenheit den falschen Eindruck erwecken, die zur Sicherstellung der Datensicherheit zu erreichenden Schutzziele zu relativieren.

Folglich beantragt die SP Schweiz, Art. 2 E-VDSG folgendermassen zu ändern:

Art. 2 Schutzziele ~~**Soweit angemessen**~~, Die Massnahmen müssen zur Gewährleistung der Datensicherheit müssen folgende Schutzziele erreichen:

2.3. Aufbewahrungsfrist der Protokolle bei automatisierten Datenbearbeitung mit hohem Risiko (Art. 3 Abs. 4 E-DSVG)

Für die SP Schweiz ist es wichtig, dass bei einer automatisierten Bearbeitung von Personendaten mit einem hohen Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen die entsprechenden Protokolle ausreichend lange aufbewahrt werden müssen, um allfällige Datenschutzverletzungen nachträglich nachvollziehen zu können und daraus für weitere solche Datenbearbeitungen präventiv die richtigen Schlüsse gezogen werden können. Vor diesem Hintergrund unterstützt die SP Schweiz die Verlängerung der Aufbewahrungsfrist dieser Protokolle gegenüber der geltenden Verordnung (vgl. Art. 10 Abs. 2) von 1 auf 2 Jahre.[5] Diese Frist darf folglich bei der Überarbeitung der Vorlage nicht gekürzt werden.

2.4. Massnahmen zur Datenminimierung in den Bearbeitungsreglementen von privaten Personen (Art. 4 Abs. 2 lit. h E-DSVG)

Für die SP Schweiz ist der Grundsatz der Datensparsamkeit ein zentrales Anliegen im Datenschutzrecht.[6] Vor diesem Hintergrund begrüssen wir es ausdrücklich, dass der Bundesrat in der totalrevidierten Datenschutzverordnung festschreiben will, dass in den Reglementen für automatisierte Bearbeitungen von privaten Personen die Massnahmen zur Datenminimierung enthalten sein müssen (siehe Art. 4 Abs. 2 lit. h)[7].

[5] Siehe Erläuternder Bericht, S. 20.

[6] Vgl. Vernehmlassungsantwort SP Schweiz zur Totalrevision des Datenschutzgesetzes, April 2017, S. 6.

[7] Vgl. Erläuternder Bericht, S. 22.

2.5. Vorgaben zur Bekanntgabe von Personendaten ins Ausland (Art. 8-12 E-VDSG)

Ganz allgemein ist es für die SP Schweiz wichtig, dass bei der Bekanntgabe von Personendaten ins Ausland der Bundesrat sicherstellt, dass der Datenschutz dabei ausreichend gewährleistet wird. Vor diesem Hintergrund halten wir die Vorgaben in der neuen VDSG zur Beurteilung eines angemessenen Datenschutzniveaus von Staaten, Gebieten oder Sektoren grundsätzlich als sachgerecht und griffig[8]. Wir fordern deshalb den Bundesrat dazu auf, bei den entsprechenden Beurteilungen diese Vorgaben konsequent anzuwenden.

2.6. Mindestanforderungen an Datenschutzklauseln und Garantien bei Bekanntgabe von Personendaten in Staaten ohne Angemessenheitsbeschluss des Bundesrates (Art. 9 E-VDSG)

Die SP Schweiz unterstützt der im Entwurf von Art. 9 E-VDSG enthaltene Vorschlag des Bundesrates, für Datenschutzklauseln und spezifische Garantien bei der Bekanntgabe von Personendaten in Staaten ohne Angemessenheitsbeschluss des Bundesrates gewisse Mindestanforderungen auf Verordnungsstufe festzuschreiben. Diese Vorgaben sind umso wichtiger, weil diese Klauseln resp. Garantien gemäss den gesetzlichen Vorgaben (vgl. Art. 16 Abs. 2 lit. b nDSG) vom EDÖB nicht genehmigt, sondern nur zur Kenntnis genommen werden müssen.[9]

2.7. Genehmigungspflicht des EDÖB von Verhaltenskodizes zur Bekanntgabe von Personen ins Ausland (Art. 12 Abs. 2 E-VDSG)

Um bei der Bekanntgabe von Personendaten ins Ausland gestützt auf unternehmensinterne Verhaltenskodizes die Sicherstellung eines angemessenen Datenschutzes wirksam zu kontrollieren zu können, begrüsst die SP Schweiz die vorgesehene Genehmigungspflicht dieser Verhaltenskodizes durch den EDÖB.[10]

---

[8] Vgl. Erläuternder Bericht, S. 25ff.

[9] Vgl. Erläuternder Bericht, S. 27.

[10] Siehe Erläuternder Bericht, S. 29.

2.8. Benachteiligungsverbot bei Verlangen der Überprüfung einer automatisierten Einzelentscheidung durch eine natürliche Person (Art. 17 E-VDSG)

Für die SP Schweiz ist es wichtig, dass Diskriminierungen bei automatisierten Einzelentscheidungen bestmöglich verhindert werden.[11] Deshalb begrüssen wir es ausdrücklich, dass der Bundesrat in der Umsetzungsverordnung festschreiben will, dass Personen, welche die Überprüfung einer automatisierten Einzelentscheidung durch eine natürliche Person verlangen dadurch nicht benachteiligt werden dürfen.[12] Damit soll richtigerweise verhindert werden, dass betroffene Person davor zurückschrecken, eine solche Überprüfung einzufordern.

2.9. Aufbewahrungsfrist für Datenschutz-Folgeabschätzung (Art. 18 E-VDSG)

Die SP Schweiz begrüsst die vom Bundesrat vorgeschlagene Aufbewahrungsfrist für die Datenschutz-Folgeabschätzung von 2 Jahren.[13] Um zu ermöglichen, dass allfällige Schwierigkeiten bei der Umsetzung dieser Datenschutz-Folgeabschätzung auch lange genug zurück noch nachvollzogen werden können, darf diese Frist nicht verkürzt werden (vgl. dazu auch oben stehend unter Ziff. 2.3.)

2.10. Informationspflicht auch über Zeitpunkt und Dauer von Datensicherheitsverletzungen (Art. 19 Abs. 3 E-VDSG)

Um den von einer Datensicherheitsverletzung betroffenen Personen zu ermöglichen, das Ausmass und das Risiko dieser Verletzung so gut wie möglich abzuschätzen, sollen die verantwortlichen Personen zusätzlich auch den Zeitpunkt und die Dauer dieser Verletzungen den betroffenen Personen und nicht wie vom Bundesrat vorgeschlagen[14] nur dem EDÖB melden müssen.

Die SP Schweiz fordert folglich, Art. 19 Abs. 3 folgendermassen zu ergänzen:

Art. 19 Meldung von Verletzungen der Datensicherheit
3 Der Verantwortliche teilt den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, **b,** e, f und g mit.

[11] Vgl. Vernehmlassungsantwort SP Schweiz zur Totalrevision des Datenschutzgesetzes, April 2017, S. 5f.

[12] Siehe Erläuternder Bericht, S. 31.

[13] Vgl. Erläuternder Bericht, S. 32.

[14] Siehe Erläuternder Bericht, S. 33.

2.11. Kostenlosigkeit des Auskunftsrechts über Datenbearbeitungen (Art. 23 E-VDSG)

Für die SP Schweiz ist es wichtig, dass das Auskunftsrecht von Personen über die Bearbeitung ihrer Personendaten in den allermeisten Fällen kostenlos wahrgenommen werden kann. Vor diesem Hintergrund verlangen wir, die ausnahmsweise Kostenbeteiligung bei unverhältnismässigem Aufwand gemäss Art. 23 Abs. 1 E-VDSG in der Praxis restriktiv anzuwenden, das Kostendach von 300.- von Art. 23 Abs. 2 nicht zu erhöhen und schliesslich keine weiteren Ausnahmen von der Kostenlosigkeit vorzusehen.[15]

2.12. Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten bei KMU mit nicht umfangreicher Bearbeitung von besonders schützenswerten Personendaten (Art. 26 lit. a E-VDSG)

Um die Sicherstellung des Datenschutzes bei der Bearbeitung von besonders schützenswerten Personendaten auch bei KMUs zu gewährleisten, wünscht sich die SP Schweiz, dass der Verzicht auf die Führung eines Verzeichnisses der Bearbeitungstätigkeiten bei nicht umfangreicher Datenbearbeitung im Sinne von Art. 26 lit. a konsequent angewandt wird und dabei insbesondere der Begriff der umfangreichen Bearbeitung solcher Daten nicht zu restriktiv ausgelegt wird.[16]

2.13. Ernennung des/der Datenschutzberater:in bei Bundesorganen (Art. 27 E-VDSG)

Für die SP Schweiz ist eine wirkungsvolle Tätigkeit der Datenschutzberater:innen in den Bundesorganen wichtig, um der Vorbildfunktion der Bundesverwaltung beim Datenschutz nachkommen zu können. Deshalb fordern wir aus den folgenden zwei Gründen, dass jedes Bundesorgan einen eigenen / eine eigene Datenschutzberaterin ernennen muss: Erstens ist jedes Bundesorgan in Bezug auf Anzahl Mitarbeitende und Anzahl bearbeitender Daten gross genug, dass es rechtfertigt, eine eigene Datenschutzberaterin / einen eigenen Datenschutzberater zu ernennen. Und zweitens kennen interne Datenschutzberater:innen die Mitarbeitende und die Betriebskultur des Bundesorgans besser als Berater:innen anderer Bundesorgane und können ihre Aufgaben deshalb effektiver wahrnehmen.[17]

---

[15] Vgl. Erläuternder Bericht, S. 37.

[16] Vgl. Erläuternder Bericht, S. 39f.

[17] Vgl. Erläuternder Bericht, S. 40.

Die SP Schweiz fordert folglich, Art. 27 folgendermassen zu ergänzen:

Art. 27 Ernennung

Jedes Bundesorgan ernennt eine Datenschutzberaterin oder einen Datenschutzberater. ~~**Mehrere Bundesorgane können gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater ernennen.**~~

Wir bitten Sie, unsere Anliegen bei der Überarbeitung der Vorlage zu berücksichtigen.

Mit freundlichen Grüssen

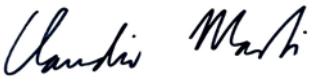
SOZIALDEMOKRATISCHE PARTEI DER SCHWEIZ

Mattea Meyer

Co-Präsidentin

Cédric Wermuth

Co-Präsident



Claudio Marti

Politischer Fachsekretär

Schweizerische Volkspartei
Union Démocratique du Centre
Unione Democratica di Centro
Partida Populara Svizra

Generalsekretariat / Secrétariat général
Postfach, CH-3001 Bern
Tel. +41(0)31 300 58 58, Fax + 41(0)31 300 58 59
gs@svp.ch, www.svp.ch, PC-Kto: 30-8828-5

Madame la Conseillère fédérale
Karin Keller-Sutter
Département fédéral de justice et police
Palais fédéral ouest
3003 Berne

Par courrier électronique :
jonas.amstutz@bj.admin.ch

Berne, le 25 octobre 2021

Révision totale de l'ordonnance relative à la loi fédérale sur la protection des données

Réponse de l'UDC Suisse à la procédure de consultation

Madame la Conseillère fédérale,

Mesdames et Messieurs,

L'UDC Suisse vous remercie de l'avoir consultée au sujet de l'objet cité en titre. Après avoir examiné les détails du projet, elle a l'avantage de se prononcer comme suit :

L'UDC regrette que la modification de l'ordonnance ne se limite pas à la stricte mise en œuvre de la loi révisée adoptée par les chambres fédérales et instaure plutôt des normes trop contraignante et manquant de souplesse. L'UDC demande le renvoi au Conseil fédéral et la présentation d'un projet moins bureaucratique et plus souple.

Alors que l'ordonnance devrait simplement mettre en œuvre la loi adoptée par le parlement, il faut constater que le Conseil fédéral souhaite utiliser sa marge de manœuvre de manière trop formaliste. Cela se remarque en matière de sous-traitance (art. 6), de communication sur la structure du groupe (art. 11) ou encore de communication des données personnelles (art. 15).

Il convient de revoir cette vision contraignante et de proposer un projet prenant moins d'initiatives en comparaison avec la loi. A ce sujet, l'obligation pour chaque office de désigner un conseiller à la protection des données va clairement trop loin (art. 27).

Schweizerische Volkspartei
Union Démocratique du Centre
Unione Democratica di Centro
Partida Populara Svizra

Generalsekretariat / Secrétariat général
Postfach, CH-3001 Bern
Tel. +41(0)31 300 58 58, Fax + 41(0)31 300 58 59
gs@svp.ch, www.svp.ch, PC-Kto: 30-8828-5

Réitérant ses remerciements de l'avoir associée à cette consultation, l'UDC Suisse vous prie de croire, Madame la Conseillère fédérale, Mesdames et Messieurs, à l'assurance de sa considération.

Avec nos meilleures salutations

UNION DÉMOCRATIQUE DU CENTRE

Le président du parti	Le secrétaire général
Marco Chiesa	Peter Keller
Conseiller aux Etats	Conseiller national

ADIDE
Association pour
le dictionnaire
des droits de l'enfant

5 chemin du Fort-de-l'Ecluse
CH-1213 Petit-Lancy / Genève
+ 41 78 759 45 38
contact@adide.ch

par courrier électronique

Office fédéral de la justice
Domaine de direction Droit public
Bundesrain 20
3003 Berne

info@bj.admin.ch
daniela.nueesch@bj.admin.ch
fanny.matthey@bj.admin.ch
noelle.koechli@bj.admin.ch

Genève, le 14 octobre 2021

Concerne : révision de l'ordonnance relative à la protection des données (OLPD)

Madame, Monsieur,

Dans le cadre de la procédure de consultation portant sur l'avant-projet d'Ordonnance relative à la loi fédérale sur la protection des données (OLPD), nous tenons à rendre l'administration fédérale une fois de plus attentive à la nécessité de formaliser certaines conditions relatives au traitement des données personnelles d'enfants et de jeunes. Non pas dans le but d'accorder à ces derniers des droits plus étendus que ceux reconnus aux « personnes concernées », mais afin de tenir compte de la responsabilité que les autorités ont d'assister les personnes mineures dans l'exercice de droits qui touchent d'extrêmement près leur vie privée et leur intimité (at. 11 et 13 al. 2 Cst).

Nous avons bien compris la teneur du courrier que Mme S. Kuster, directrice suppléante de l'OFJ, nous a adressé à ce propos le 19 mars dernier, mais nous ne partageons pas ce point de vue.

Le 27 septembre dernier, le Comité des droits de l'enfant des Nations Unies a publié les recommandations spécifiques destinées au gouvernement helvétique. Il demande aux autorités de développer des normes qui protègent la vie privée des enfants en relation avec le traitement de leurs données personnelles (CRC/C/CHE/CO/5-6, para. 24).

Les risques d'atteinte aux droits personnels et les difficultés d'exercice de leurs propres droits par les personnes mineures doivent être corrélés avec un devoir spécial d'attention et de diligence imposé aux entreprises et aux organes qui traitent des données personnelles. Si ni la loi, ni l'ordonnance ne contiennent d'allusion à ces particularités, chacun de ces intervenants s'en remettra soit au laisser-faire, soit à l'improvisation. Le résultat final en sera une application disparate des garanties auxquelles chacune et chacun a légitimement droit, chaque individu étant contraint de sans cesse s'adapter à des conditions différant d'une entreprise à l'autre ou d'un contexte à l'autre.

Nous prions instamment l'administration fédérale de ne pas se satisfaire de cette situation. Les autorités ont une obligation de sollicitude vis-à-vis des populations démunies en raison de leur âge, de leur immaturité ou de leurs déficits cognitifs. Leur responsabilité doit se concrétiser par la voie réglementaire, en définissant plus précisément les modalités du devoir d'informer (art. 13 ss. de l'avant-projet) et les conditions d'exercice de ses droits par la personne concernée lorsqu'elle est mineure (chapitre 3 de l'avant-projet). Vu l'importance de l'enjeu, le recours à des recommandations et à des directives est insuffisant.

./..

Sur les deux points susmentionnés, le RGPD contient des clauses intéressantes, dont il est possible de s'inspirer, même dans le nommer.

Nous vous remercions une fois encore de vous pencher sur ces propositions, qui feront du nouveau droit suisse de la protection des données un droit qui parle aussi des enfants et aux enfants, et qui tient compte de leur besoin de protection et d'encouragement (art. 11 Cst.).

Veuillez agréer, Madame, Monsieur, nos salutations distinguées.

pour L'ADIDE

Marie-Françoise Lücker-Babel
Dr. iur.
auteure du Dictionnaire des droits de l'enfant

Copies : M. A. Lobsiger, Préposé fédéral à la protection des données et à la transparence, 3003 Berne, adrian.lobsiger@edoeb.admin.ch
Mme Astrid Wüthrich, OFAS, Vice-directrice, responsable du domaine «Familles, générations et société», 3003 Berne, astrid.wuethrich@bsv.admin.ch

Association of Foreign Banks in Switzerland
Verband der Auslandsbanken in der Schweiz
Association des banques étrangères en Suisse
Associazione delle banche estere in Svizzera

foreign banks . in switzerland .

Federal Department of Justice and Police
3003 Bern

jonas.amstutz@bj.admin.ch

Zürich, 14 October 2021

AFBS Comments: draft Data Protection Ordinance

Dear Madam, Dear Sir

The Association of Foreign Banks in Switzerland AFBS thanks for the invitation to comment on the draft Ordinance on Data Protection. It wishes to outline a series of points, which are of particular concern to the foreign banks in Switzerland. The points are listed in the document attached to this letter.

Beyond the points listed in the document we would like to attract your attention on the fact that the wording of Art 3 Par 1 of the Law provides for a very broad scope of application. It obliges processors abroad to fully align with Swiss regulation if they wish to service data owners in Switzerland. That can be contrary to an open and competitive market, restrict choice for Swiss data owners and impose high cost. Therefore, we suggest clarifying the scope of Art 3 Par 1 of the Law and to align it with the territorial scope as outlined in Article 3 of the GDRP.

The comments have been elaborated in several meetings among member banks, in which the Law, draft Ordinance and their implementation have been at the centre stage.

The AFBS also contributed to the comments drafted by the Swiss Bankers' Association, which it fully endorses.

We remain at your disposal for any questions you may have and are would be pleased to discuss specific points in detail.

We thank you in advance for your attention.

Best Regards

ASSOCIATION OF FOREIGN BANKS IN SWITZERLAND

Raoul Würgler
Secretary General

Florian Specht
Scientific Advisor

Usteristrasse 23 · CH-8001 Zürich
T +41 44 224 40 70 · F +41 44 221 00 29
www.afbs.ch · info@afbs.ch

Data Protection Ordinance

This is a list of points that were identified by the representatives of the AFBS members during a Roundtable in August 2021. Speakers from Oberson Abels SA presented the draft ordinance and discussed points of potential interest to the foreign banks.

Art 3 Par 1

The wording in German is more restrictive than in French and Italian. The German text restricts the specific requirement to automated processing of personal data, which the French and Italian version do not. This lack of consistency needs to be avoided as it entails legal uncertainty. The three language versions need to clarify that logging obligations apply only in case of presence of high risk with automated processing of personal data, but not in any case. Therefore, the text in French and Italian needs to be amended.

[1]Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko …

[1]Lorsque l'analyse d'impact sur la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement automatisé de données personnelles envisagé présente encore un risque élevé …

[1]Se dalla valutazione d'impatto sulla protezione dei dati emerge che, nonostante i provvedimenti previsti dal titolare del trattamento automatizzato dei dati di persona, sussiste ancora un rischio elevato per la personalità o i diritti fondamentali delle persone interessate, …

Art 3 Par 4

The Paragraph lacks legal basis and shall therefore be deleted. There is no point in restricting access to protected data which is, in any case, governed by the DPA and therefore subject to clear rules. Data controllers shall not be precluded from using the protocols as long as they respect the requirements of the revised DPA.

Art 4

The Article requires the drafting of a registry of processing activities. A similar requirement is defined in Art 12 DPA. There is no plausible reason for the Ordinance to repeat obligations outlined in the Law already. Doing so bears the risk of inconsistency, confusion, and contradiction.

Furthermore, there is no legal provision requesting the drafting of a registry of processing of private persons' data. The listing contained of registration duties of Art 12 applies to all instances of data processing. This is sufficient.

The entire article shall be deleted as it duplicates Art 12 DPA.

Art 8

Art 16 DPA identifies the Federal Council in charge of identifying those jurisdictions / international organisations which offer adequate measures of data protection and therefore qualify for data disclosure. Therefore, Art 8 DPO shall specify that it is the Federal Council that needs to perform the assessment of the jurisdictions / international organisations and that it needs to take into account the ensuing list of criteria for the adequateness assessment.

It must be clear that the Federal Council's decision regarding adequateness of the measures of data protection of a country / international organisation is definitive and does not trigger further control measures by the exporter.

[1]Zur Beurteilung, ob Personendaten ins Ausland bekanntgegeben werden dürfen, prüft der Bundesrat, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleisten. Er berücksichtigt dabei namentlich folgende Kriterien:

…

[6]Der Bundesrat konsultiert den EDÖB ~~wird~~ … ~~konsultiert.~~

[1]Pour l'évaluation de l'admissibilité du transfert de données à l'étranger, le Conseil fédéral examine, si un Etat, un territoire, un ou plusieurs secteurs déterminés dans un Etat, ou si un organisme international garantit un niveau de protection adéquat. Il prend en compte notamment les critères suivants:

…

[6]Le Conseil fédéral consulte le PFPDT ~~est consulté~~ ….

[1]Per valutare se la comunicazione dei dati all'estero è ammissibile, il Consiglio federale esamina, se uno Stato, un territorio, uno o più settori di uno Stato o di un organismo internazionale garantisce una protezione adeguata dei dati. Prende ~~vanno segnatamente presi~~ in considerazione i seguenti criteri:

…

[6]Il Consiglio federale consulta l'IFPDT ~~è consultato~~ ….

Art 13

The data processor cannot be expected to comply with an obligation of information as extensive as drafted in Art 13 Par 1. It does not have information on the subjects to be informed and may even not be aware of what information it is legally entitled to provide and to whom. Requesting the data processor to provide information which the controller can potentially provide itself furthermore bears the risk of duplicate information being issued. This can lead to contradictions.

Paragraph 2 shall be deleted. It is difficult to understand and does not add value. There is no information on what a machine-readable pictogramme is.

A separate paragraph shall provide clarity on how to provide information to the concerned persons on the processing of personal data. This requires legal clarity. The topic is complex, various solutions are available. Clear and unequivocal guidance in Law and Ordinance can contribute to assure clarity and consistent practice. This brings legal certainty which is in the interest of all.

Therefore, Art 13 shall be worded as follows:

[1]Der Verantwortliche teilt ~~und der Auftragsbearbeiter teilen~~ die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit.

~~[2]Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~

[3]Der Verantwortliche kann die Information auf einer Website verfügbar machen. Die Website muss einfach zugänglich sein und der Verantwortliche teilt den betroffenen Personen deren Adresse mit.

[1]Le responsable du traitement ~~et le sous-traitant~~ communique~~nt~~ les informations sur la collecte de données personnelles de manière concise, compréhensible et facilement accessible.

~~[2]Lorsque l'information se fait en combinaison de pictogrammes, ceux-ci doivent être lisibles par machine s'ils sont présentés par voie électronique.~~

[3]Le responsable du traitement peut mettre à disposition l'information sur un site web. Le site web doit être facile d'accès et le responsable communique son adresse aux personnes concernées.

[1]Il titolare del trattamento ~~e il responsabile~~ comunica~~no~~ le informazioni sull'ottenimento di dati personali in forma precisa, comprensibile e facilmente accessibile.

~~[2]Se le informazioni sono comunicate in combinazione con pittogrammi rappresentati in forma elettronica, questi ultimi devono essere leggibili a macchina.~~

[3]Il responsabile del trattamento può mettere a disposizione l'informazione su un sito web. Questo sito web dev'essere facile d'accesso e il responsabile del trattamento comunica il suo indirizzo alle persone colpite.

Art 18

The Article needs to clarify that the storage in writing / in print is not the only way, but that alternative means of text storage are available for the documentation of the data protection impact assessment.

Furthermore, there is no legal basis for the impact assessment to be stored for two years beyond end of processing.

Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in einer anderen durch Text nachweisbaren Form festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~

Le responsable du traitement consigne par écrit ou sous une autre forme de texte traçable l'analyse d'impact relative à la protection des données personnelles. ~~Elle est conservée pendant deux ans après la fin du traitement des données.~~

Le responsable du traitement consigne par écrit l'analyse d'impact relative à la protection des données personnelles. ~~Elle est conservée pendant deux ans après la fin du traitement des données.~~

Il titolare del trattamento redige per scritto o in un altro formato di testo rintracciabile la valutazione d'impatto sulla protezione dei dati. ~~Quest'ultima è conservata per due anni dopo la fine del trattamento.~~

Art 19 Par 3

The data controller must not be obliged to communicate extensively and in detail about the remediation measures adopted to mitigate future incidents. This information belongs to the realm of the data controller. Its dissemination merely facilitates future attacks.

[3]Der Verantwortliche teilt den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e und f ~~und g~~ mit.

[3]Le responsable du traitement communique à la personne concernée, dans un langage simple et compréhensible, au moins les informations visées à l'al. 1, let a, e et f ~~et g~~.

[3]Il titolare del trattamento comunica alla persona interessata in una lingua semplice e comprensibile almeno le informazioni di cui al capoverso 1 lettera a, e e f ~~e g~~.

Art 19 Par 5

The Paragraph 5 lacks legal basis. It is therefore to be deleted.

If it is to be maintained, it needs to clarify that the data controller can only provide information on points it is aware of. The data controller cannot be expected to perform investigation beyond its own realm

[5]Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss ~~alle~~ die mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.

[5]Le responsable du traitement document les violations. La documentation contient ~~tous~~ les faits relatifs aux incidents, à leurs effets et aux mesures prises. Elle est conservée pendant au moins trois ans à compter de la date d'annonce, au sens de l'al. 1.

[5]Il titolare documenta le violazioni. La documentazione contiene ~~tutti~~ i fatti legati agli eventi, le loro conseguenze e i provvedimenti adottati. Deve essere conservata per almeno tre anni dalla notifica secondo il capoverso 1.

Art 48

The present legislation is complex and impacts a broad range of services within the individual firms. The individual measures to be adopted are dependent on each other; there are links between different prescriptions. It imposes extensive amendments of processes and procedures. To assure a holistic approach is possible when implementing the new regulation, the date of entry into force should leave sufficient time for transition and be the same for the entire text.

Entry into force of the DPA and DPO shall be on 1 January 2023 at the earliest.

AGVS | UPSA
Auto Gewerbe Verband Schweiz
Union professionnelle suisse de l'automobile
Unione professionale svizzera dell'automobile

Elektronische Einreichung:
fanny.matthey@bj.admin.ch
daniela.nueesch@bj.admin.ch

Bern, 27. September 2021 // os

Revision der Datenschutzverordnung

Stellungnahme des Auto Gewerbe Verband Schweiz (AGVS)

Sehr geehrte Frau Matthey
Sehr geehrte Frau Nüesch
Sehr geehrte Damen und Herren

Der Auto Gewerbe Verband Schweiz (AGVS) vertritt seit 1927 die Interessen von heute rund 4'000 Garagenbetrieben in der Schweiz und dem Fürstentum Liechtenstein.

Wir bedanken uns für die Gelegenheit, zu dem im Titel genannten Thema wie folgt Stellung nehmen zu dürfen. Am 25. September 2020 hat das Parlament – nach langen Debatten – die Totalrevision des Schweizer Datenschutzgesetzes (revDSG) verabschiedet. Dieses ist international abgestimmt, um dem EU-Standard (DSGVO) Rechnung zu tragen, enthält im Wesentlichen daher keine Swiss Finishes. Damit schafft das Gesetz Rechtssicherheit für Schweizer Unternehmen, welche sich (auch) an die Bestimmungen der DSGVO halten müssen. **Der Entwurf der Verordnung zum Datenschutzgesetz (E-VDSG) gefährdet die gewonnene Rechtssicherheit durch zahlreiche Regelungen, welche weit über diejenigen der DSGVO hinausgehen. Zudem wurden Punkte in die E-VDSG aufnenommen, welche während den Debatten aus dem Gesetzesentwurf entfernt wurden.**

Wir bitten Sie, den Entwurf dahingehend zu überarbeiten, dass sämtliche Swiss Finishes und Widersprüche zum revDSG beseitigt werden. Die Verordnung hat sich auf Konkretisierungen des Gesetzes zu beschränken und darf insbesondere nicht Regelunge aufzustellen, welche bewusst nicht in das Gesetz aufgenommen wurden (z.B. Art. 16 E-VDSG). Unsere nachfolgenden Forderungen und Formulierungsvorschläge in Bezug auf einzelne Artikel des Entwurfs sollen Ihnen bei der Überarbeitung dienen. Alle aufgeführten Punkte sind aus unserer Sicht grundsätzlich zwingend zu berücksichtigen (Prio 1: dunkelorange, Prio 2: hellorange, Prio 3: weiss).

Bei allfälligen Rückfragen stehen wir Ihnen gerne zur Verfügung

Urs Wernli
Zentralpräsident

Pierre Daniel Senn
Vizepräsident

mobilcity.ch

AGVS/UPSA
Wölflistrasse 5, Postfach 64, 3000 Bern 22
Telefon 031 307 15 15, Fax 031 307 15 16
info@agvs.ch, www.agvs.ch

Artikel	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag
Generell	Entgegen ihrer Natur als reine ***Ausführungs***verordnung zum Datenschutzgesetz enthält die E-VDSG Regelungen, welche über eine blosse Konkretisierung des revDSG hinausgehen.	Die VDSG hat ausschliesslich die Konkretisierung des revDSG zum Zweck (vgl. Erläuterungen, S. 9). Sie darf darüber hinaus keine zusätzlichen eigenen Regelungen vorsehen. Dies führte zu einer eigentlichen Parallelgesetzgebung.	Konsequente Streichung aller mit dem E-VDSG eingeführten **Swiss Finishs** (vgl. nachfolgend). Ergänzung der Titel in der Verordnung mit einer Verweisung auf die entsprechende gesetzliche Grundlage. Z.B.: „Art. 1 Grundsätze (Art. 8 Abs. 3 DSG)“
	Die zusätzlich aufgestellten Regelungen entbehren nicht nur einer Rechtsgrundlage im Gesetz, wo der Gesetzgeber teilweise bewusst anders entschieden hat, sondern gehen auch über das Niveau der DSGVO hinaus. Diese **Swiss Finishs** stehen aber im Widerspruch zur expliziten Zielsetzung des Gesetzgebers und auch des BJ, wonach Kompatibilität mit der DSGVO geschafft werden sollte (Erläuterungen, S. 10).	Wie das BJ in den Erläuterungen (S. 10) selbst ausführt, soll durch Kompatibilität mit der DSGVO Rechtssicherheit für Unternehmen geschaffen werden, welche sich an die DSGVO halten. Das gelingt freilich nicht, wenn die VDSG gegenüber dem revDSG (neue) **Swiss Finishs** einführt. Im Gegenteil, damit sind Doppelspurigkeiten und Widersprüche vorprogrammiert.	
1	Berücksichtigung des Implementierungsaufwands statt der -kosten als Kriterium aufnehmen.	Die Erläuterungen zur Berücksichtigung der Implementierungskosten als Kriterium bei der Beurteilung der Angemessenheit sind u.E. unpräzise (vgl. Erläuterungen, S. 16). Entgegen diesen Ausführungen sind die Implementierungskosten gemäss E-VDSG 1 I b bei der Beurteilung der Frage, ob eine Massnahme angemessen ist, zu berücksichtigen, und nicht erst, wenn es darum geht, sich für eine von mehreren angemessenen Massnahmen zu entscheiden. Zudem ist nicht allein auf die Implementierungs*kosten*, sondern generell auf den Implementierungs*aufwand* abzustellen. Das sollte in der Verordnung entsprechend präzisiert werden.	1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a.–c. […]; d. Implementierungs~~kosten~~*aufwand*. ~~2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.~~ **Eventualiter:** 1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:

	Streichung der Pflicht zur Überprüfung in angemessenen Abständen. **Eventualiter:** Pflicht zur Überprüfung der Massnahmen in angemessener *Weise*	Die Pflicht zur Überprüfung in angemessenen Abständen nach VDSG 1 II hat keine Grundlage im revDSG. **Eventualiter:** Wenn, dann sind die Massnahmen infolge risikobasierten Ansatzes nicht in angemessenen *Abständen*, sondern vielmehr in angemessener *Weise* zu überprüfen. Denn die Frage, ob eine Kontrolle nötig ist, hängt insbesondere davon ab, ob sich die Risiken geändert haben. Zeitliche Aspekte sind irrelevant.	a.–c. […]; d. Implementierungs~~kosten~~*aufwand*. 2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessene~~n~~*r* ~~Abständen~~ *Weise* zu überprüfen.
3	Die Protokollierungspflicht nach VDSG 3 ist zu streichen. **Eventualiter:** Einschränkung auf Fälle, wo ohne Protokollierung nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden (vgl. auch geltender Art. 10 Abs. 1 VDSG).	Die Protokollierungspflicht nach VDSG 3 hat keine Grundlage im revDSG und widerspricht dem risikobasierten Ansatz. Auch „hohen" Risiken ist mit den im Einzelfall *adäquaten Massnahmen* zu begegnen. Die DSGVO sieht keine Protokollierungspflicht vor. Es handelt sich daher um einen **Swiss Finish**. Auf einer Dokumentationspflicht, wie sie im VE-DSG vorgesehen war, wurde aufgrund der Eingaben in der Vernehmlassung verzichtet bzw. sie wurde durch die Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen ersetzt. Diese geht weiter als die bisherige Pflicht zur Anmeldung der Datensammlung beim EDÖB. Es müssen neu alle Bearbeitungen in einem Verzeichnis aufgeführt sein. Es nicht erforderlich, an der Protokollierungspflicht festzuhalten.	**Streichung von VDSG 3**, zumindest für den Privatbereich. **Eventualiter:** 1 Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht *und kann sonst nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden,* protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. 2 […] 3 […] 4 […]

		Die Einführung der Protokollierungspflicht als Teil der Datensicherheit hätte stossende Auswirkungen: Falls trotz gegebenen Voraussetzungen keine DSFA durchgeführt wird, so hat dies gemäss revDSG *keine* Sanktion zur Folge. Wird hingegen eine DSFA durchgeführt, aber in der Folge gegen die allfällige Protokollierungspflicht (als Teil der Datensicherheit) verstossen, so ist das sanktionsbedroht. Der Verantwortliche hat die vorgängig Stellungnahme des EDÖB einzuholen, wenn sich aus der DSFA ergibt, dass eine geplante Bearbeitung trotz Massnahmen ein hohes zur Folge hat. Der EDÖB kann dem Verantwortlichen bei etwaigen Einwänden (angemessene) ebenfalls Massnahmen vorschlagen.	
4	Die Pflicht zur Erstellung eines Reglements nach VDSG 4 ist zu streichen. **Eventualiter:** Falls an dieser Regelung festgehalten werden sollte, müsste zumindest präzisiert werden, dass die Angaben gemäss Abs. 2 einzig in Bezug auf Bearbeitungen gemacht werden müssen, welche unter Art. 1 Abs. 1 lit. a und/oder b fallen.	Die Pflicht zur Erstellung eines Reglements nach VDSG 4 I hat keine Grundlage im revDSG und widerspricht dem risikobasierten Ansatz. Auch „hohen" Risiken ist mit den im Einzelfall *adäquaten* Massnahmen zu begegnen. Die DSGVO sieht keine Pflicht zur Erstellung eines Reglements vor. Es handelt sich daher um einen **Swiss Finish**. Auf einer Dokumentationspflicht, wie sie im VE-DSG vorgesehen war, wurde aufgrund der Eingaben in der Vernehmlassung verzichtet bzw. sie wurde durch die Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen ersetzt. Diese geht weiter als die bisherige Pflicht zur Anmeldung der Datensammlung beim EDÖB.	**Streichung von VDSG 4**, zumindest für den Privatbereich.

		Es müssen neu alle Bearbeitungen in einem Verzeichnis aufgeführt sein. Es nicht erforderlich, an der praxisfernen Pflicht zur Erstellung eines Reglements festzuhalten.	
6	Unklar, was die Ausführungen auf S. 24 der Erläuterungen zu den Anforderungen an den Inhalt des ADV gemäss Art. 22 Abs. 3 DSGVO bezwecken, zumal diese in Art. 6 E-VDSG nicht vorgesehen sind.	Diese Ausführungen suggerieren, dass der ADV gemäss VDSG 6 den inhaltlichen Anforderungen der DSGVO genügen müsse. Hierfür findet sich indes keine gesetzliche Grundlage. Auch die E-VDSG enthält keine inhaltlichen Vorgaben.	Klarstellung im Erläuterungsbericht, dass die VDSG – anders als die DSGVO – keinen Mindestinhalt an den ADV vorschreibt.
	Streichung der Pflicht zur Sicherstellung einer vertrags- oder gesetzesgemässen Bearbeitung.	„Sicherstellung" der vertrags- und gesetzesgemässen Bearbeitung ist nicht möglich. Analog DSGVO 28 I kann der Verantwortliche nur, aber immerhin verpflichtet werden, nur Auftragsbearbeiter zu beauftragten, welche durch angemessene Massnahmen die Bearbeitung im Einklang mit den Anforderungen des revDSG und den Schutz der Rechte der Betroffenen gewährleisten.	1 Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. ~~Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.~~ *Er arbeitet nur mit Auftragsbearbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen so durchgeführt werden, dass die Bearbeitung im Einklang mit den Anforderungen der Schweizer Datenschutzgesetzgebung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.* 2 ~~Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.~~ 3 Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich *oder in einer anderen Form, die den Nachweis durch Text ermöglicht,* genehmigt hat.
	Streichung von Abs. 2, weil der Auslandtransfer separat geregelt ist.	Abs. 2: Auslandtransfers sind separat geregelt (E-VDSG 8), weshalb für diese Regelung keine Notwendigkeit besteht. Sollte an dieser Regelung festgehalten werden, so wäre im letzten Satz zu präzisieren, dass „andernfalls ein geeigneter Datenschutz gemäss Art. 16 Abs. 2 revDSG zu gewährleisten ist."	
	Präzisierung des Begriffs „schriftlich", der auch „in Text nachweisbare Formen" umfasst.	Abs. 3: „Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	

10	Der Empfänger kann nicht verpflichtet werden, „die schweizerischen Datenschutzvorschriften“ einzuhalten. Das ist im Erläuterungsbericht klarzustellen.	Im Erläuterungsbericht (S. 28) ist festgehalten, dass der Empfänger verpflichtet werden müsse, „die schweizerischen Datenschutzvorschriften“ einzuhalten. Das ist unzutreffend; er muss die Standardklauseln einhalten, nicht jedoch Schweizer Datenschutzrecht. So verlangt auch E-VDSG 6 II, dass der Auftragsbearbeiter „gleichwertige“ Bestimmungen einhalten muss.	Klarstellung im Erläuterungsbericht, dass der Empfänger nicht verpflichtet werden muss, „die schweizerischen Datenschutzvorschriften“ einzuhalten.
	Ersatz des Begriffs „Sicherstellung“ durch „darauf hinwirken“.	Der Exporteur kann nicht „sicherstellen“, dass der Empfänger die Standarddatenschutzklauseln beachtet; er kann nur, aber immerhin darauf hinwirken.	1 Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um ~~sicherzustellen~~ *darauf hinzuwirken*, dass die Empfängerin oder der Empfänger diese beachtet. *Die Angemessenheit der Massnahmen richtet sich nach den Umständen im konkreten Fall und dem Stand der Technik.* 2 […]
	Präzisierung, dass sich die Angemessenheit der geforderten Massnahmen nach den Umständen im konkreten Einzelfall richte und die Anforderungen insb. dann höher seien, wenn es sich um besonders schützenswerte Personendaten handle.	Dies ist in den Erläuterungen (S. 28) unter Hinweis auf das BJ entsprechend festgehalten und sollte zur Klarstellung auch in die Verordnung einfliessen. Der risikobasierte Ansatz bei der Beurteilung von Datentransfers in Länder ohne angemessenen Datenschutz auf Grundlage der SCC ist zu bejahen. Allerdings ist dieser Ansatz mit Blick auf die Praxishinweise der EU-Behörden keinesfalls selbstverständlich. Entsprechend bedarf es einer Klarstellung in der Verordnung zur Schaffung von Rechtssicherheit.	
NEU	Präzisierung des räumlichen Anwendungsbereichs des revDSG (Auswirkungsprinzip, Art. 3 I):	Gemäss revDSG 3 I gilt das Gesetz für Sachverhalte, die sich in der Schweiz auswirken auch wenn sie im Ausland veranlasst werden. Weder das Gesetz noch die Verordnung halten fest, ob an die Auswirkungen weitere Anforderungen zu stellen sind. Eine solche qualifizierte Auswirkung (Spürbarkeit) ist erforderlich, um Übertreibungen bei der extraterritorialen Anwendung des Schweizer Datenschutzrechts vorzubeugen. Hierzu ist eine Regelung analog zum Marktortprinzip gemäss DSGVO aufzunehmen.	*Folgende Sachverhalte, die im Ausland veranlasst werden, wirken sich in der Schweiz aus:* *a. das Angebot von Waren oder Dienstleistungen gegenüber betroffenen Personen in der Schweiz;* b. *die Beobachtung des Verhaltens von betroffenen Personen, soweit ihr Verhalten in der Schweiz erfolgt.*

13	Richtigstellung, dass keine „Basisinformationen“ auf der ersten Kommunikationsstufe mitgeteilt werden müssen.	Das revDSG sieht nicht vor, dass die Betroffenen die „wichtigsten Informationen“ auf der „ersten Kommunikationsstufe“ erhalten müssen (vgl. aber Erläuterungen, S. 30). Vielmehr hält revDSG 19 I fest, die Information müsse „angemessen“ erfolgen. Daraus folgt, dass das die Mitteilung von den jeweiligen Umständen abhängig ist. Dabei sind auch Informationsinteresse und die Erwartungen des Betroffenen zu berücksichtigen: Während er damit rechnen mag, dass sich in einem Vertrag ein Hinweis auf den die Datenschutzerklärung findet, ist ein solcher auf Visitenkarten, E-Mails oder Briefpapier nicht üblich. Sollte sich eine Person dafür interessieren, kann ihr zugemutet werden, die Webseite des betreffenden Unternehmens zu konsultieren. Darum darf es nicht erforderlich sein, in Alltagssituationen – wie bei einer Terminvereinbarung, am Schalter – explizit auf die Datenschutzerklärung hinweisen zu müssen (s. Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 99). Zudem wäre ohnehin unklar, welches die „wichtigsten Informationen“ sind.	Richtigstellung im Erläuterungsbericht, dass den Betroffenen keine „Basisinformationen“ auf der ersten Kommunikationsstufe mitgeteilt werden müssen und dass auch das Informationsinteresse der Betroffenen im Einzelfall zu berücksichtigen ist.
	Streichung der gesetzlich nicht vorgesehenen Informationspflicht des Auftragsbearbeiters.	Der Auftragsbearbeiter hat gemäss revDSG keine Informationspflicht (vgl. revDSG 19). Eine solche kann nicht in der VDSG eingeführt werden.	**Streichung von Art. 13 VDSG** **Eventualiter:** ~~1~~ Der Verantwortliche *~~und der Auftragsbearbeiter teilen~~ teilt* die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit. *Als leicht zugänglich gilt insbesondere die Information, welche auf der Webseite des Verantwortlichen abrufbar ist.* ~~2 Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~
	Streichung der unpräzisen Vorgaben für eine angemessene Information. Streichung der unklaren Anforderungen an Piktogramme.	Weil Piktogramme ohnehin nur ergänzend verwendet werden dürfen, sind daran keine zusätzlichen Anforderungen zu stellen. Zumal aufgrund der Erläuterungen nicht klar ist, was mit „maschinenlesbar“ gemeint ist.	

15	Die Informationspflicht bei der Bekanntgabe von Personendaten ist zu streichen.	Diese Informationspflicht entbehrt einer Grundlage im revDSG. Auf die Richtlinie (EU) 2016/680 (Schengen-RL) ist für den Privatbereich nicht abzustellen. Die DSGVO sieht keine entsprechend Pflicht vor. Eine Umsetzung ist nicht erforderlich und schafft einen **Swiss Finish**. Der Auftragsbearbeiter ist gemäss revDSG wie bereits erwähnt nicht Adressat der Informationspflicht. Keine Notwendigkeit: Der Verantwortliche hat bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten.	**Streichung von Art. 15.**
16	Die Informationspflicht über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten ist zu streichen.	Diese Informationspflicht entbehrt einer Grundlage im revDSG. Diese Pflicht wurde im Vorentwurf des DSG vorgeschlagen, im Rahmen der Vernehmlassung jedoch wieder gestrichen. Sie darf entsprechend nicht über die VDSG wieder eingeführt werden. Keine Notwendigkeit: Der Verantwortliche hat bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten.	**Streichung von Art. 16.**

18	Analog DSGVO 35 IV soll der EDÖB eine Liste erstellen und publizieren, welche Bearbeitungen enthält, für die eine bzw. keine DSFA zu erfolgen hat. Alternativ oder kumulativ sind Kriterien zu nennen, wonach ermittelt werden kann, ob eine DSFA durchzuführen ist oder nicht. „Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	Ohne Kriterien und/oder Liste mit Beispielen von Bearbeitungen, die eine DSFA erfordern bzw. nicht erfordern, besteht eine grosse Rechtsunsicherheit.	*1 Der Beauftragte erstellt eine Liste mit Bearbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Er kann zusätzlich eine Liste mit Bearbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.* *2* Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich *oder in einer anderen Form, die den Nachweis durch Text ermöglicht,* festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~
	Die Aufbewahrungsfrist ist zu streichen.	Die Dokumentationspflicht gemäss VDSG 18 entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Zudem besteht der Anreiz, der Dokumentationspflicht nicht nachzukommen, da diese – im Gegensatz zu einer Verletzung der Datensicherheit – nicht strafbar ist. Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelungen einen **Swiss Finish** darstellen.	
	Der Begriff der Schriftlichkeit ist zu präzisieren.	„Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	

19	Die Auslegung des Begriffs „voraussichtlich“ ist falsch und zu korrigieren.	„Voraussichtlich“ heisst nicht, dass „in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen kann, eine Meldung erfolgen muss“ (so die Erläuterungen, S. 32). Der Begriff „voraussichtlich“ setzt vielmehr voraus, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko führt.	Richtigstellung im Erläuterungsbericht, dass in Fällen, wo das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, nicht gemeldet werden muss, sondern nur dann, wenn die Verletzung der Datensicherheit **höchstwahrscheinlich** zu einem hohen Risiko führt.
	Streichung der in der Verordnung gegenüber dem Gesetz zusätzlich eingeführten Mindestangaben bei einer Meldung einer Verletzung der Datensicherheit.	Gemäss revDSG 24 II hat der Verantwortliche in der Meldung einer Verletzung der Datensicherheit „mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen zu [nennen]“. Die E-VDSG sieht weitere Mindestangaben vor. Die DSGVO sieht keine Angabe von Zeitpunkt und Daher der Verletzung vor. Es handelt sich daher um einen **Swiss Finish**.	1 Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit: a. die Art der Verletzung; ~~b. soweit möglich den Zeitpunkt und die Dauer;~~ ~~c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;~~ ~~d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;~~ e.-g. […] 2 […] *3* ~~Der~~ *Falls der* Verantwortliche *verpflichtet ist, die* ~~teilt den~~ betroffenen Personen *zu informieren, so teilt er ihnen* in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit. 4 […] ~~5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.~~
	Streichung der über das Gesetz hinausgehenden generellen Pflicht, die betroffene Person zu informieren.	E-VDSG 19 II geht über revDSG 20 IV hinaus. Während das Gesetz eine Information der betroffenen Person nur vorschreibt, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt, sieht die Verordnung vor, dass der Verantwortliche den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mitteilt.	
	Streichung der gesetzlich nicht vorgesehenen Dokumentationspflicht nach VDSG 19 V.	Dokumentationspflicht nach VDSG 19 V entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie nach der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor. Es handelt sich daher um einen **Swiss Finish**. Falls an der Dokumentationspflicht festgehalten werden sollte, ist zu präzisieren, dass nur meldepflichtige Verletzungen aufzubewahren sind.	

20	Die Auskunftserteilung sollte nicht nur schriftlich, sondern auch in einer anderen durch Text nachweisbaren Form möglich sein.	In den Erläuterungen (S. 34) wird festgehalten: „Es kann hier ferner präzisiert werden, dass zur schriftlichen Form auch die elektronische Form gehört." Diese Präzisierung ist in die Verordnung aufzunehmen.	1 […] 2 Die Auskunft wird in der Regel schriftlich *oder in einer Form, die den Nachweis durch Text ermöglicht,* erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat. 3-4 […] *5 Die betroffene Person hat keinen Anspruch auf Herausgabe von Dokumenten, selbst wenn diese Personendaten enthalten sollten.* ~~5 Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.~~
	Aufnahme der Präzisierung, dass der Begriff „Daten als solche" insbesondere auch eine Auskunft in aggregierter Form zulässt.	In den Erläuterungen (S. 35) wird ausgeführt: „Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Die mündliche Mitteilung von Informationen, zum Beispiel am Telefon, ist ebenfalls möglich, sofern die betroffene Person eingewilligt hat." Es besteht im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten bzw. Unterlagen. Vielmehr ist die Mitteilung nach entsprechender Debatte vom Gesetzgeber bewusst beschränkt worden auf die bearbeiteten Personendaten „als solche" (revDSG 25 II b). Damit soll namentlich auch die Auskunft in aggregierter Form ermöglicht werden. Dies sollte zwecks Präzisierung in der Verordnung verankert werden.	

	Dokumentationspflicht nach VDSG 20 V ist zu streichen.	Dokumentationspflicht nach VDSG 20 V entbehrt einer gesetzlichen Grundlage(vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen **Swiss Finish** darstellen. Die Regelung ist ferner unnötig, da aufgrund der Beweislast ohnehin im Interesse des Verantwortlichen mit Dokumentation den Nachweis erbringen zu können.	
22	Der Fristenbeginn ist zu präzisieren.	Präzisierung erforderlich: Wenn aus dem Auskunftsbegehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.	1 Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen*. Wenn aus dem Begehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.* 2 […]
23	Erhöhung der Beteiligung an den Kosten für eine Auskunftserteilung.	Eine wesentliche Erhöhung der Beteiligung des Betroffenen ist angezeigt, weil der geltende Betrag von CHF 300.00 regelmässig in keinem Verhältnis zum Aufwand steht.	1 […] 2 Die Beteiligung beträgt maximal *5'000.00* Franken. 3 […]
24	Klarstellung, dass „Datenportabilität" kein Zwang zu standardisierten Datenbearbeitungssystemen beinhaltet.	Die „Datenportabilität" wurde erst im Rahmen der parlamentarischen Debatte eingeführt. Entsprechend enthält die Botschaft keine Ausführungen dazu. Die Verordnung muss hier Konkretisierungsarbeit leisten.	*1 Das Recht der betroffenen Person, sie betreffende Personendaten vom Verantwortlichen heraus zu verlangen oder durch diesen an einen anderen Verantwortlichen übertragen zu lassen, begründet für den Verantwortlichen nicht die Pflicht, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten.*

			2 […]
26	Es ist zu präzisieren, dass sich die allfällige Pflicht eines KMU zur Führung eines Verzeichnisses nicht auf sämtliche Bearbeitungen erstreckt, sondern auf diejenigen Bearbeitungen beschränkt ist, welche die Voraussetzung(en) triggern.	Der Bundesrat hat gemäss revDSG 12 V Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses vorzusehen für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und deren Datenbearbeitung ein „geringes Risiko“ mit sich bringt. Gemäss E-VDSG 26 bedeutet ein geringes Risiko, dass weder „umfangreich besonders schützenswerte Personendaten bearbeitet“ werden noch „ein Profiling mit hohem Risiko durchgeführt“ wird. Alle anderen Bearbeitungen bringen im Umkehrschluss ein geringes Risiko mit sich. Durch Präzisierung, dass sich die Pflicht zur Führung eines Verzeichnisses ausschliesslich auf diejenigen Bearbeitungen erstreckt, welche die Voraussetzung triggern, kann sowohl dem Schutz der betroffenen Personen als auch den Bedürfnissen der KMU angemessen Rechnung getragen werden (vgl. auch das Positionspapier des EDSA zu Art. 30 Abs. 5 DSGVO).	*1* Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. […] b. […] *2 Ist eine Voraussetzung nach Abs. 1 Bst. a und/oder b erfüllt, so ist die Verzeichnispflicht auf diejenige bzw. diejenigen Bearbeitungen beschränkt, welche dieser bzw. diesen Voraussetzung bzw. Voraussetzungen zugrunde liegen.* *3 Das Bearbeitungsverzeichnis ist schriftlich, oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu führen.*
	Es ist ferner zu präzisieren, dass das Verzeichnis nicht schriftlich, sondern auch in anderer Form, die den Nachweis durch Text ermöglicht, z.B. elektronisch, geführt werden kann.	Damit ist klargestellt, dass das Verzeichnis auch elektronisch geführt werden kann.	

Insertion Suisse
Arbeitsintegration Schweiz
Inserimento Svizzera

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per E-Mail an:
jonas.amstutz@bj.admin.ch

Bern, 12. Oktober 2021

Stellungnahme von Arbeitsintegration Schweiz zur Vernehmlassung: Ausführungsrecht zum Datenschutzgesetz (revidierte Verordnung über den Datenschutz)

Sehr geehrte Damen und Herren

Arbeitsintegration Schweiz (AIS) nimmt gerne Stellung zu den Ausführungsbestimmungen zum Datenschutzgesetz. AIS ist der nationale Dachverband der sozialen und beruflichen Integration. Sie vereint gesamtschweizerisch mehr als 230 Mitgliedsorganisationen, die eine Vielzahl an Integrationsdienstleistungen anbieten.

Grundzüge der vorliegenden Stellungnahme

Die vorliegende Vernehmlassungsantwort fokussiert auf die für die Institutionen und Strukturen für Menschen mit Unterstützungsbedarf relevanten Punkte der vom Bundesrat vorgeschlagene VDSG-Revision.

In der Stellungnahme wird in erster Linie darauf geachtet, dass die vom Bundesrat vorgeschlagenen Umsetzungsmodalitäten des revidierten Datenschutzgesetzes möglichst schlank, praxisnah und anwendungsfreundlich für die Betriebe bleiben. Das ist nicht selbstverständlich im Rahmen eines Gesetzgebungsprozesses, der nicht besonders darauf ausgerichtet ist: Dieser strebt offensichtlich vor allem eine sehr genaue und umfangreiche Einhaltung des Datenschutzes an.

Des Weiteren beantragt die vorliegende Vernehmlassungsantwort eine möglichst konkrete, zugängliche und auch finanziell günstige Unterstützung der Betriebe durch die zuständigen staatlichen Stellen – vor allem durch den Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Die in der Stellungnahme vertretenen Standpunkte berücksichtigen gleichwohl die Wichtigkeit eines zielführenden Datenschutzes: Allgemein wird davon ausgegangen, dass die Betriebe oftmals heikle Daten bearbeiten, deren Bekanntgabe ein hohes Risiko für die betroffenen Personen von Unterstützungs-leistungen aufweisen können; deswegen soll an einem strikten Datenschutz nicht gerüttelt werden.

Auch wird in der vorliegenden Vernehmlassungsantwort beantragt, dass grob umrissene Begriffe und Abgrenzungen präziser umschrieben werden – dies im Sinne einer möglichst klaren Umsetzungshilfe für die betroffenen Betriebe.

Relevante Bestimmungen der E-VDSG für die ambulanten und stationären Betriebe für Personen mit Unterstützungsbedarf

E-VDSG	Kommentar	Beantragte Neuformulierung
Art. 1 Abs. 1	Die vorgeschlagene Umschreibung ist im Grundsatz zu begrüssen. Sie ergänzt und konkretisiert sinnvollerweise Artikel 8 Absatz 1 nDSG. Zu begrüssen ist, dass sie möglichst schlank und angesichts der stetigen technischen Entwicklungen flexibel, praxisnah und anwendungsfreundlich gehalten worden ist. Weil sie sehr allgemein formuliert ist, braucht es aber entsprechenden Deutungs- und Umsetzungshilfen für die Praxis.	- Es müssen seitens EDÖB möglichst bald Dokumente geschaffen werden, welche den Betrieben die Praxisumsetzung vereinfachen.
Art. 1 Abs. 2	Die Abstände zwischen den vorzunehmen Überprüfungen sollten präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Was genau „angemessene Abstände" sind, hängt selbstverständlich von den Besonderheiten des konkreten Anwendungsfalls ab (S. 17 im erläuternden Bericht: «[…] bei der Bestimmung der Massnahmen selbstredend die Umstände des Einzelfalls massgeblich [bleiben]»). Während die Datenbearbeiter inhaltlich grossen Freiraum für die Bestimmung ihrer konkreten Massnahmen brauchen, sollte zeitlich zumindest eine konkrete Anforderung gelten, um die Sicherheit zu gewährleisten. Als sinnvoll erscheint uns eine mindestens jährliche Überprüfung.	[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen, jedoch mindestens einmal pro Jahr zu überprüfen.
Art. 2	Diese präzise Auflistung der Schutzziele macht Sinn: Sie stellt eine praxisorientierte ‚Gedächtnisstütze' für die Verantwortlichen und die Auftragsbearbeiter dar, was im Rahmen ihrer Konkretisierung zu berücksichtigen ist. Wichtig ist eine gute Anwendbarkeit in der Praxis (Seite 17 des Berichts: „In Anwendung der Verhältnismässigkeit sind ausgehend [… von dieser Auflistung der Schutzziele] die organisatorischen und technischen Massnahmen des Einzelfalls zu bestimmen.").	- Für eine optimale und kostengünstige Umsetzung ist darauf zu achten, dass Schweizer Unternehmen einen guten und kostengünstigen Zugang zum EDÖB erhalten (vgl. auch Art. 45 Abs. 2).

	Gleichzeitig zeigt diese Auflistung die Komplexität der Anforderungen an eine gesetzkonforme Datenbearbeitung und -sicherheit auf - mit dem damit verbundenen Aufwand. Aus diesem Grund ist eine möglichst konkrete und für Schweizer Betriebe auch unentgeltliche Unterstützung der Datenschutzverantwortlichen durch die zuständigen Behörden (insbesondere das EDÖB), vorzusehen. So können die Umsetzungskosten für Wirtschaft und Gesellschaft minimiert und angemessene Datensicherheit auf allen Ebenen geschaffen werden.	
Art. 3	Welche „Massnahmen" im vorliegenden Rahmen berücksichtigt werden sollen und ob ein Risiko als hoch oder begrenzt eingeschätzt werden soll, dürfte in der Praxis oftmals schwierig zu beurteilen sein, denn Artikel 8 nDSG führt auch keine präziseren Anhaltspunkte über die Art der infrage stehenden Massnahmen an. Dies entspricht zwar einer flexiblen, bedarfsorientierten und dem neusten technischen Stand angepassten Umsetzung des Datenschutzes, macht aber dessen Realisierung in der Praxis schwierig. In diesem Sinne ist die Präzisierung der Inhalte der Protokollierung (gemäss Abs. 3) an sich konsequent und kongruent. Sie weist aber einen hohen Detaillierungsgrad auf, der einen entsprechend hohen Umsetzungsaufwand, eine Unübersichtlichkeit und mögliche Verwechslungs-risiken mit sich bringt. Es ist festzustellen, dass gerade bei der *automatisierten* Bearbeitung von Personendaten die Anforderung einer detaillierten Protokollierung einen beträchtlichen Teil der Vorteile der Automatisierung beraubt: Der zeitliche und administrative Aufwand wird dadurch erheblich vergrössert. Trotzdem erscheint uns eine Protokollierung richtig, sofern keine anderen Massnahmen das gleiche Ziel mit weniger Aufwand erreichen können. *Antrag:* Alternativen zur Protokollierung als Massnahmen zum Datenschutz sollen im E-VDSG ausdrücklich vorgesehen und auch aufgezählt werden – wie etwa die physische/räumliche Sicherung der Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.	In Art. 3 Abs. 1 müssen Alternativen zur im Entwurf vorgesehenen (komplexen) Protokollierung – ausdrück-lich vorgesehen und auch aufgezählt werden, nament-lich Zugriffskontrollen, die physische/räumliche Sicherung der Daten, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.

Art. 4 Abs. 2	Weil in sehr vielen Fällen eine automatisierte Bearbeitung von besonders schützenswerten Personendaten erfolgt, sind die von dieser Bestimmung gestellten Anforderungen als zu aufwendig und vielfach unnötig zu qualifizieren. Sie bringen für die betroffenen Datenbearbeiter unangemessen hohe Kosten mit sich. Deswegen ist diese Auflistung zu kürzen. Die Buchstaben d, e und j sollen ersatzlos gestrichen werden, weil sie unnötige zusätzliche Anforderungen und Präzisierungen darstellen, die den administrativen Aufwand für die Betriebe verschärfen, ohne dass daraus ein entsprechender Nutzen entsteht. Buchstabe i soll gekürzt werden: Er weist einen Detaillierungsrad mit entsprechenden Umsetzungskosten auf, der in keinem vernünftigen Verhältnis zu seinem Nutzen steht. Hingegen werden Buchstaben a, b, c, f und g ausdrücklich begrüsst, da sie zentrale Massnahmen zur Gewährleistung der Datensicherheit darstellen. Ihre Einhaltung genügt, um dem Datenschutz gerecht zu werden. Auch Buchstabe h wird begrüsst, weil eine stets angestrebte Datenminimierung das beste Mittel darstellt, um sowohl den Schutz der Privatsphäre als auch die Verminderung des mit jeglichem Datenbearbeitung verbundenen administrativen Aufwands zu erreichen.	[2] Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. ~~zur internen Organisation~~; e. ~~zur Herkunft der Personendaten und zur Art ihrer Beschaffung~~; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den ~~Datenbearbeitungs-verfahren, insbesondere den~~ Verfahren bei der Speicherung, ~~Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung,~~ Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. ~~zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf~~

		~~Datenherausgabe oder -übertragung.~~
Art. 4 Abs. 3	Analog obigem Antrag zu Art. 1 Abs. 2 sollten auch hier die zeitlichen Abstände zwischen den vorzunehmenden Aktualisierungen präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Deswegen wird hier beantragt, dass die Aktualisierungen mindestens einmal jährlich stattfinden: Dieser Zeitabstand stellt eine präzise, zugleich realistische und daher auch anwendungsfreundliche Leitplanke dar.	[3] Die private Person muss das Reglement ~~regelmässig~~ in angemessenen Abständen, jedoch mindestens einmal pro Jahr, aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.
Art. 6 Abs. 2	Die in dieser Bestimmung gestellten Anforderungen an die Verantwortlichen betreffend dem DSG nicht unterstellten Datenbearbeiter sind offensichtlich zu hoch. Von einem Verantwortlichen kann vernünftigerweise nicht verlangt werden, dass er Kenntnis der vielen potenziell relevanten Gesetzesbestimmungen und der möglichen Abhilfe-Lösungen hat. Wenn schon ist es die Pflicht von Gesetzgeber und Verwaltung, den Datenschutz so auszugestalten, dass dieser – wo nötig und sinnvoll – überall für alle Betroffenen gleichermassen gilt. Diese Pflicht den einzelnen Verantwortlichen aufzubürden, wie der Bundesrat es vorschlägt, führt zu enormer Unsicherheit und Aufwand. Deswegen ist dieser Absatz ersatzlos zu streichen.	~~[2] Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.~~
Art. 8 Abs. 1	Aus der Formulierung dieser Bestimmung geht überhaupt nicht klar hervor, wer für die Beurteilung der Angemessenheit des Datenschutzes in einem anderen Staat zuständig ist. Aus dem erläuternden Bericht hingegen schon (S. 25 ff): Der Bundesrat ist zuständig. Der Klarheit wegen sollte diese Zuständigkeit in Art. 8 E-VDSC eindeutig geregelt werden, sonst besteht das Risiko, dass sich private Akteure dafür verantwortlich halten – was ihren Aufwand erheblich erhöhen würde.	[1] Werden Personendaten ins Ausland bekanntgegeben, so müssen ~~bei der~~ anlässlich einer regelmässigen Beurteilung durch den Bundesrat, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden: […]

Art. 8 Abs. 3	Die Abstände zwischen den vorzunehmenden Beurteilungen sollen präziser angegeben werden. Deswegen wird auch hier beantragt, dass die Beurteilungen mindestens einmal jährlich stattfinden müssen.	[3] Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch, jedoch mindestens einmal pro Jahr, neu beurteilt.
Art. 9 Abs. 1	Die von Art. 9 E-VDSG gestellten Anforderungen erreichen ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Zwar sind diese Anforderungen für das Ziel des Datenschutzes konsequent, sie verursachen aber hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden. Nämlich Bst. b, c, g, h sowie i sind offensichtlich unnötig; Ihre Anwendung wäre unverhältnismässig aufwändig. Die anderen Bestimmungen genügen, um die «spezifischen Garantien» zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.	[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen die Datensicherheit mindestens die folgenden Punkte regeln: […] ~~b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen~~ ~~c. die Art und der Zweck der Bekanntgabe von Personendaten;~~ ~~[…]~~ ~~g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger;~~ ~~h. die Massnahmen zur Gewährleistung der Datensicherheit;~~ ~~i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;~~ […]

Art. 10	Wir begrüssen, dass der EDÖB eine Liste von Standard-Datenschutzklauseln veröffentlicht, um den Aufwand für die Betroffenen zu reduzieren und eine gewisse Vereinheitlichung der Schutzklauseln zu erreichen.	-
Art. 15	Bei der Anwendung dieser Bestimmung ist darauf zu achten, dass die Anforderungen an den Detaillierungsgrad der mit der Bekanntgabe von Personendaten verbundenen Informationen nicht zu umfangreich ausfallen soll. Meistens werden sich die zum Datenschutz benötigten Informationen aus den Daten oder den Begleitumständen selbst ergeben.	-
Art. 18	Nach unserer Einschätzung reicht es aus, wenn *nach Beendigung der Datenbearbeitung* (was bei entsprechenden Gerichtsverfahren bereits Jahre dauern kann) eine Aufbewahrung für ein Jahr statt zwei Jahre stattfindet.	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während ~~zwei Jahren~~ einem Jahr nach Beendigung der Daten-bearbeitung aufbewahrt werden.
Art. 20	Die vorgesehene Dreifachlösung (schriftlich, mündlich oder durch Einsichtnahme an Ort und Stelle) erscheint sinnvoll. So kann für Menschen mit gewissen Krankheiten oder einer Beeinträchtigung eine geeignete Lösung gefunden werden. Für gewisse Fälle, wie an Demenz erkrankte oder weitere kognitiv beeinträchtigte Menschen dürfte die Anforderung in Abs. 3 kaum einzuhalten sein. Deshalb ist für diese Fälle eine Präzisierung aufzunehmen.	[3] Die Auskunft muss für die betroffene Person verständlich sein, soweit dies im Rahmen ihrer kognitiven Fähigkeiten möglich ist.
Art. 22	Die Frist von 30 Tagen ab Eingang des Begehrens um Dateneinsicht erscheint uns vernünftig. Es stellt sich einzig die Frage, ob nicht die Gerichtsferien berücksichtigt werden sollten (namentlich die Sommermonate und Weihnachten, wegen vieler Absenzen).	
Art. 23	Bei unverhältnismässig aufwändigen Auskunftserteilungen erscheint uns die auf 300 Franken angesetzte Obergrenze als zu tief. Wenn damit mehrere Arbeitstage an Aufwand anfallen, wäre nicht einmal ein Bruchteil der Kosten auf die Gesuchstellenden gedeckt. Der Betrag sollte – auch gerade als Schutz vor querulatorischen Begehren – auf mindestens 1'000 Franken	[1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist.

	erhöht werden, um tatsächlich abschreckend wirken zu können.	[2] Die Beteiligung beträgt maximal ~~300~~ 1'000 Franken.
Art. 25	Die Datenschutzgesetzgebung weist eine hohe Komplexität auf; deshalb sind ihre Anforderungen in der Praxis nicht immer einfach einzuhalten. Deswegen ist es sehr sinnvoll, Datenschutzberatende einzusetzen und die konkreten Modalitäten zu deren Einsatz im Sinne dieser Bestimmung festzulegen. Die Inhalte sind zu begrüssen, wie sie in dieser Bestimmung vorgeschlagen sind.	-
Art. 26 Bst. a + b	Die hier definierte und sinnvolle Ausnahme einer Pflicht zur Führung eines Bearbeitungsverzeichnisses würde bei zahlreichen Betrieben nicht zur Anwendung kommen, weil • in vielen Fällen die Betriebe besonders schützenswerte Personendaten in grossem Umfang bearbeiten; • aus einer Interpretation von Art. 20 Abs. 4, Art. 26 Abs. 3, Art. 31 Abs. 2 Bst. b nDSG hervorgeht, dass Art. 26 eVSDG auch Betriebe mit weniger als 250 Mitarbeitenden angewendet werden soll, wenn sie einem Konzern zugehören, der insgesamt mindestens 250 Mitarbeitende beschäftigt. Um Rechtssicherheit zu gewährleisten und keinen unnötigen Aufwand für kleinere Betriebe (namentlich im Sozial- und Gesundheitsbereich) zu schaffen, ist eine Anpassung wichtig. Während wir die Unterstellung von Teilen der Konzerne nachvollziehen können, erscheint uns die «Bearbeitung von besonders schützenswerten Daten in grossem Umfang» als zu wenig präzise Konkretisierung. Wir beantragen deshalb eine Präzisierung, was unter «grossem Umfang» zu verstehen ist, nach unserer Ansicht wäre die Schwelle etwa bei 1'000 Datensätzen festzusetzen. Diesfalls erhält auch die Führung eines Verzeichnisses aber auf freiwilliger Basis mehr Gewicht, sie kann insbesondere bei regelmässiger Bearbeitung von Personendaten eine nützliche und einfache Tätigkeitsunterstützung darstellen: Dadurch können das Beibehalten eines Überblicks der Bearbeitungstätigkeiten und auch die Einhaltung anderer Verpflichtungen erleichtert werden.	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. Es werden umfangreich (mindestens 1'000 Datensätze) besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.
Art. 45 Abs. 2	Aus unserer Sicht ist unverständlich, warum eine nationale Behörde für die Dienstleistung im Bereich des der ganzen	[2bis] Wenn die Bearbeitung besonders schützenswerte

	Bevölkerung dienenden Datenschutzes solch hohe Kostensätze von 150 bis 350 Franken verlangen soll. Dies schreckt geradezu ab, diese sinnvollen Dienstleistungen zu beziehen, welche einer guten Umsetzung der Gesetzgebung dienen. Es ist unverständlich, dass für die Dienstleistungen der Verwaltung solche Preise wie bei spezialisierten Anwaltskanzleien verrechnet werden. Als besonders stossend empfinden wir solche Honorare zulasten von Leistungserbringern, wenn diese besonders schützenswerte Personendaten bearbeiten: Es wäre falsch, diese mit hohen Stundensätzen vom Bezug der sinnvollen Unterstützung seitens EDÖB abzuschrecken. Diese Betriebe sind denn mit den neuen Regelungen auch besonders stark herausgefordert und eine gute Umsetzung ist im Interesse der Behörden und der Bevölkerung. Diese Belastung ist umso fragwürdiger, als die öffentliche Hand im Endeffekt und in vielen Fällen, die dadurch verursachten Defizite ausgleichen soll: Mit einer Hand wegnehmen, was mit der anderen gegeben wird, macht betriebswirtschaftlich keinen Sinn und verursacht einen sinnlosen administrativen Aufwand. Die Zutrittsschwelle zum EDÖB ist niedrig zu halten, ganz besonders auch zur Überprüfung der Angemessenheit von Kodizes (Art. 59 Abs. 1 Bst. a nDSG) oder die Genehmigung von Standarddatenschutzklauseln (Art. 59 Abs. 1 Bst. b nDSG). Im Sinne einer rechtmässigen Umsetzung der komplexen neuen Datenschutzgesetzgebung sollte das Anrufen des EDÖB nicht durch das Erheben von Gebühren entgegengewirkt werden. Ganz besonders für den Bereich der Gesundheitsbetriebe muss deshalb eine Ausnahme geschaffen werden, welche vernünftige Stundenansätze vorsieht.	Personendaten betrifft, wird auf die Erhebung von Kosten verzichtet. Alternativ: 2bis Wenn die Bearbeitung besonders schützenswerte Personendaten betrifft, gilt ein Stundenansatz von 50 bis 100 Franken.

Insertion Suisse
Arbeitsintegration Schweiz
Inserimento Svizzera

Wir danken Ihnen für die Gelegenheit zur Vernehmlassung und für die gebührende Berücksichtigung unserer Stellungnahme im Rahmen Ihrer weiteren Bearbeitung dieses Geschäfts.

Freundliche Grüsse

Fatoş Bağ
Geschäftsleiterin
Arbeitsintegration Schweiz

Kontakt für Rückfragen:
Fatoş Bağ
Tel. 031 321 56 39
fatos.bag@arbeitsintegrationschweiz.ch

Association Suisse des Délégués
à la Protection des Données (ASDPO)
asdpo.swiss
contact@asdpo.swiss

Genève, le 14 octobre 2021

Département fédéral
de justice et police
A l'att. de Monsieur
Jonas Amstutz
jonas.amstutz@bj.admin.ch

Réponse de l'ASDPO à la consultation sur l'avant-projet d'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Monsieur,

Pour donner suite à l'ouverture le 23 juin 2021 de la consultation concernant la révision de l'ordonnance sur la protection des données, l'Association Suisse des Délégués à la Protection des Données (ASDPO) a l'honneur de vous faire parvenir ci-dessous sa prise de position sur l'avant-projet mentionné en objet.

Conformément à ses statuts, l'ASDPO poursuit notamment les buts suivants qui légitiment sa participation à ladite consultation :

- promouvoir et développer la fonction de délégués (ou conseillers) à la protection des données en Suisse ;
- participer à des consultations relatives à l'évolution de la législation sur la protection des données.

Nous restons à votre disposition pour toute question que vous pourriez avoir et vous invitons à vous adresser directement comité de l'association au moyen de l'adresse e-mail susmentionnée.

En vous remerciant de l'attention que vous porterez à ce document, nous vous prions d'agréer, Monsieur, l'expression de notre considération distinguée.

François Charlet
Président

Nesrin Keles & Isabelle Hering
Membres du comité

Annexe : prise de position du 13 octobre 2021 de l'ASDPO sur l'avant-projet d'OLPD

Prise de position du 13 octobre 2021 de l'ASDPO sur l'avant-projet d'OLPD

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 1 Principes [1] Pour savoir si les mesures techniques ou organisationnelles visant à garantir la sécurité des données sont adaptées au risque, les critères suivants sont pris en considération : a. la finalité, la nature, l'étendue et les circonstances du traitement des données ; b. la probabilité d'une violation de la sécurité des données et son impact potentiel sur les personnes concernées ; c. l'état de la technique ; d. les coûts de mise en œuvre. [2] Les mesures sont réexaminées à des intervalles appropriés pendant toute la durée du traitement.	Ces principes sont bienvenus. Cependant, au vu de l'art. 8 al. 3 nLPD, on s'attendait à ce que le Conseil fédéral édicte un catalogue de mesures minimales de sécurité, et non une liste de critères à considérer pour que les entités soumises à la nLPD décident des mesures de sécurité à appliquer. En outre, la violation de ces exigences minimales de sécurité est punissable pénalement selon l'art. 61 let. c nLPD. Le fait de ne pas détailler précisément quelles sont ces exigences pose un réel problème en regard de l'art. 1 CP. Il n'est pas clair quand la responsabilité pénale sera engagée.	Fournir une réelle liste de mesures minimales de sécurité, qui peuvent être sélectionnées dans la liste de l'art. 2.
Art. 2 Objectifs de protection Dans la mesure du possible, les mesures de sécurité des données doivent permettre d'atteindre les objectifs de protection suivants : a. contrôle de l'accès aux données : l'accès des personnes autorisées est limité aux données personnelles dont elles ont besoin pour accomplir leurs tâches ; b. contrôle de l'accès aux locaux et installations : l'accès aux locaux et aux installations utilisées pour le traitement de données personnelles est refusé aux personnes non autorisées ; c. contrôle des supports de données : les personnes non autorisées ne peuvent pas lire, copier, modifier, déplacer ou supprimer des supports de données ; d. contrôle de mémoire : les personnes non autorisées ne peuvent ni introduire de données personnelles dans la mémoire ni consulter, modifier ou effacer des données personnelles enregistrées ;	Lettre d : contrôle de mémoire, le terme « mémoire » ne paraît pas en adéquation avec la description de l'objectif de protection. Des mesures de sécurité des données doivent permettre d'atteindre les objectifs dans tous les cas et non « dans la mesure du possible » car cela laisse une trop grande marge de manœuvre pour la mise en place de la sécurité des données.	Remplacer « mémoire » par « intégrité » semble plus correct d'un point de vue de sécurité informatique. Modifier la phrase introductive : *« En considérant les principes énoncés à l'art.1, les mesures de sécurité des données doivent permettre d'atteindre les objectifs de protection suivants… »*

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
e. contrôle d'utilisation : les personnes non autorisées ne peuvent pas utiliser les systèmes de traitement automatisé de données personnelles au moyen d'installations de transmission ; f. contrôle du transport : les personnes non autorisées ne peuvent pas lire, copier, modifier ou effacer des données personnelles lors de leur communication ou lors du transport de supports de données ; g. contrôle de la saisie : l'identité des personnes saisissant ou modifiant des données personnelles dans le système automatisé, ainsi que les données saisies ou modifiées et le moment de leur saisie ou modification peuvent être vérifiés ; h. contrôle de la communication : il doit être possible de vérifier à qui sont communiquées des données personnelles à l'aide d'installations de transmission ; i. restauration : la disponibilité des données personnelles et l'accès aux données personnelles peuvent être rapidement rétablis en cas d'incident physique ou technique ; j. toutes les fonctions du système doivent être disponibles (disponibilité), les dysfonctionnements éventuels doivent être signalés (fiabilité) et les données personnelles stockées ne doivent pas pouvoir être endommagées par des dysfonctionnements du système (intégrité des données) ; k. détection : les violations de la sécurité des données doivent pouvoir être rapidement détectées et des mesures doivent pouvoir être prises pour réduire ou éliminer les conséquences.		
Art. 3 Journalisation 1 Lorsque l'analyse d'impact sur la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, le responsable du traitement privé et son sous-traitant journalisent au moins les opérations suivantes :	Al. 4 : pourquoi un délai de deux ans ? De manière générale, d'où proviennent les délais introduits dans le P-OLPD et ne serait-il pas pertinent de les uniformiser ? P. ex. en adoptant partout un délai de 5 ans identique à celui de la prescription pénale de l'art. 66 nLPD. La différence de traitement entre les responsables du traitement privés et les organes fédéraux n'a pas lieu d'être et ne peut être objectivement justifiée.	Harmoniser tous les délais de conservation à 5 ans. Supprimer la différence entre les responsables du traitement privés et les organes fédéraux.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
enregistrement, modification, lecture, communication, effacement ou destruction. 2 Lors du traitement automatisé de données personnelles, l'organe fédéral et son sous-traitant journalisent au moins les opérations suivantes : enregistrement, modification, lecture, communication, effacement ou destruction. 3 La journalisation doit fournir des informations sur la nature du traitement, l'identité de la personne qui a effectué le traitement, l'identité du destinataire et le moment auquel le traitement a eu lieu. 4 Les procès-verbaux de journalisation sont conservés durant deux ans, séparément du système dans lequel les données personnelles sont traitées. Ils sont accessibles aux seuls organes ou personnes chargés de vérifier l'application des dispositions de protection des données personnelles ou de rétablir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ils ne sont utilisés qu'à cette fin.		
Art. 4 Règlement de traitement des personnes privées 1 Le responsable du traitement et son sous-traitant établissent un règlement pour les traitements automatisés en cas : a. de traitement de données sensibles à grande échelle, ou b. de profilage à risque élevé. 2 Le règlement de traitement contient au moins des indications sur : a. la finalité du traitement ; b. les catégories de personnes concernées et les catégories de données personnelles traitées ; c. la durée de conservation des données personnelles ou les critères utilisés pour déterminer cette durée ; d. l'organisation interne ; e. l'origine des données personnelles et leur mode de collecte ;	Aucune base légale dans la nLPD ne permet d'édicter cet article.	Supprimer la disposition.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
f. les mesures techniques et organisationnelles visant à garantir la sécurité des données ; g. les autorisations d'accès, ainsi que sur la nature et l'étendue de cet accès ; h. les mesures prises pour la minimisation des données ; i. les procédures de traitement des données, notamment les procédures, d'enregistrement, de rectification, de communication, de conservation, d'archivage, de pseudonymisation, d'anonymisation et d'effacement ou de destruction des données ; j. la procédure d'exercice du droit d'accès et du droit à la remise ou à la transmission des données personnelles. 3 La personne privée actualise régulièrement le règlement et le met à la disposition du conseiller à la protection des données sous une forme qui lui est intelligible.		
Art. 5 Règlement de traitement des organes fédéraux 1 L'organe fédéral responsable et son sous-traitant établissent un règlement pour les traitements automatisés en cas : a. de traitement de données sensibles ; b. de profilage ; c. de traitement de données personnelles au sens de l'art. 34, al. 2, let. c, LPD ; d. d'accès aux données personnelles accordé à des cantons, des autorités étrangères, des organisations internationales ou des personnes privées ; e. d'ensembles de données interconnectés, ou f. d'exploitation d'un système d'information ou de gestion d'ensembles de données conjointement avec d'autres organes fédéraux. 2 Le règlement de traitement contient au moins les indications prévues à l'art. 4, al. 2. 3 L'organe fédéral responsable actualise régulièrement le règlement et le met à la disposition du conseiller à la	Aucune base légale dans la nLPD ne permet d'édicter cet article.	Supprimer la disposition.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
protection des données sous une forme qui lui est intelligible, ainsi qu'à la disposition du Préposé fédéral à la protection des données et à la transparence (PFPDT), si celui-ci en fait la demande.		
Art. 6 Modalités 1 Le responsable du traitement qui confie un traitement de données personnelles à un sous-traitant demeure responsable de la protection des données. Il s'assure que les données soient traitées conformément au contrat ou à la loi. 2 Lorsqu'un sous-traitant n'est pas soumis à la LPD, le responsable du traitement s'assure que d'autres dispositions légales garantissent une protection équivalente. A défaut, il s'assure qu'une telle protection est garantie par des clauses contractuelles. 3 Lorsque le responsable de traitement est un organe fédéral, le sous-traitant ne peut sous-traiter le traitement des données à un tiers que si l'organe fédéral l'a approuvé par écrit.	Al. 1 : il est problématique que les données doivent être traitées conformément au contrat ou à la loi. Si le contrat déroge à la loi, le sous-traitant pourrait ne pas respecter la loi. Al. 2 : l'obligation de garantir la sécurité des données figure déjà dans la loi. En outre, des mesures contractuelles seules peuvent ne pas suffire. Enfin, quelles sont les situations dans lesquelles un sous-traitant n'est pas soumis à la nLPD, au vu du champ d'application territorial de cette dernière (art. 3 al. 1 nLPD) ? Al. 3 : la sous-sous-traitance devrait être conditionnée à un accord écrit également pour les responsables du traitement privé.	Al. 1 : supprimer la seconde phrase. Al. 2 : « Lorsqu'un sous-traitant n'est pas soumis à la LPD, le responsable du traitement s'assure que d'autres dispositions légales garantissent une protection équivalente. A défaut, il s'assure qu'une telle protection est garantie par des clauses contractuelles, ainsi que des mesures organisationnelles et techniques. » Al. 3 : « ~~Lorsque le responsable de traitement est un organe fédéral~~, le sous-traitant ne peut sous-traiter le traitement des données à un tiers que si le responsable de traitement l'a approuvé par écrit. »
Art. 7 Information du conseiller à la protection des données de l'organe fédéral L'organe fédéral informe sans délai le conseiller à la protection des données de la conclusion d'un contrat avec un sous-traitant ou de l'autorisation de sous-traiter le traitement des données à un tiers. Il informe également le conseiller à la protection des données si des problèmes surviennent dans le respect des exigences légales ou contractuelles de protection des données personnelles.	/	/
Art. 8 Évaluation du niveau de protection adéquat des données personnelles d'un État étranger ou d'un organisme international	Al. 3 : la fréquence de la réévaluation périodique est manquante. Se calquer sur le RGPD.	Al. 3 : "Le niveau de protection dans l'Etat, le territoire, le ou les secteurs déterminés dans un Etat, ou l'organisme international concerné, est réévalué

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
1 En cas de communication de données personnelles à l'étranger, les critères suivants doivent notamment être pris en compte pour évaluer si un État, un territoire, un ou plusieurs secteurs déterminés dans un Etat, ou si un organisme international garantit un niveau de protection adéquat : a. les engagements internationaux de l'État ou de l'organisme international en matière de protection des données personnelles ; b. le respect des droits humains ; c. la législation applicable en matière de protection des données, de même que sa mise en œuvre et la jurisprudence y relative ; d. la garantie effective des droits des personnes concernées et des voies de droit ; e. le fonctionnement effectif d'une ou de plusieurs autorités indépendantes chargées de la protection des données dans l'État concerné, ou auxquelles un organisme international est soumis, et disposant de pouvoirs et de compétences suffisants. 2 L'évaluation peut tenir compte des appréciations effectuées par des organismes internationaux ou des autorités étrangères chargées de la protection des données personnelles. 3 Le niveau de protection dans l'État, le territoire, le ou les secteurs déterminés dans un État, ou l'organisme international concerné, est réévalué périodiquement. 4 Lorsqu'il est constaté, à l'issue de l'évaluation visée à l'al. 3, ou lorsque les informations disponibles révèlent qu'un État, un territoire, un ou plusieurs secteurs déterminés dans un État, ou un organisme international n'assure plus un niveau de protection adéquat, la décision au sens de l'art. 16, al. 1, LPD est modifiée, suspendue ou abrogée. La nouvelle décision n'a pas d'effet sur la communication des données déjà effectuée. 5 Les États, les territoires, les secteurs déterminés dans un États, et les organismes internationaux avec	Al. 4 : indiquer que la nouvelle décision n'a pas d'effet sur les données déjà transférées à l'étranger est erroné. Le responsable du traitement doit réévaluer la situation lorsqu'une décision d'adéquation est modifiée, suspendue ou abrogée, et généralement sélectionner un autre mécanisme s'il souhaite continuer à transférer des données. Les données déjà transférées l'ont certes été sous un régime d'adéquation, mais elles sont désormais traitées dans un État qui n'offre plus de niveau de protection adéquat, ce qui peut porter atteinte aux droits de la personnalité des personnes concernées. Il n'est pas acceptable de tolérer cette situation. Quelle est la procédure applicable à la prise de décision ? Les États concernés peuvent-ils recourir ?	périodiquement, mais au maximum tous les quatre ans." Al. 4 : supprimer la dernière phrase.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
un niveau de protection adéquat sont mentionnés à l'annexe 1. 6 Le PFPDT est consulté avant toute décision portant sur l'adéquation.		
Art. 9 Clauses de protection des données d'un contrat et garanties spécifiques 1 Les clauses de protection des données d'un contrat au sens de l'art. 16, al. 2, let. b, LPD et les garanties spécifiques au sens de l'art. 16, al. 2, let. c, LPD portent au moins sur les points suivants : a. l'application des principes de licéité, de bonne foi, de proportionnalité, de finalité et d'exactitude ; b. les catégories de données communiquées et de personnes concernées ; c. le type et la finalité de la communication des données personnelles ; d. le nom des Etats de destination ; e. le nom des organismes internationaux de destination ; f. les conditions applicables à la conservation, l'effacement et la destruction des données personnelles ; g. les destinataires habilités à traiter les données ; h. les mesures garantissant la sécurité des données personnelles ; i. les conditions applicables à la communication des données à un autre Etat étranger ou à un autre organisme international ; j. l'obligation pour les destinataires d'informer les personnes concernées par le traitement des données ; k. les droits de la personne concernée, en particulier : 1. de demander l'accès à ses données personnelles, 2. de s'opposer au traitement des données personnelles, 3. de demander la rectification, l'effacement ou la destruction de données personnelles, 4. de saisir en justice une autorité indépendante. 2 Le responsable du traitement prend les mesures adéquates pour s'assurer que le destinataire respecte	Al. 1 : dans l'énumération, il manque un point sur le droit d'audit de l'exportateur des données vis-à-vis de l'importateur (mesure nécessaire pour être en mesure de contrôler le niveau de protection), ainsi qu'un point sur l'obligation d'annonces des violations de la sécurité des données.	Al. 1 let. a : ajouter le principe de transparence/information (cf. art. 16 et 17 nLPD) Al. 1 let. h : "les mesures techniques et organisationnelles" Al. 1 let. k : ajouter le droit à la remise des données (cf. art. 28 et 29 nLPD) Al. 1 : ajouter une lettre m sur le droit d'audit et une lettre n sur l'annonce des violations de la sécurité des données.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
les clauses de protection des données d'un contrat ou les garanties spécifiques. 3 Une fois les clauses de protection des données d'un contrat ou les garanties spécifiques annoncées au PFPDT, le devoir d'information du responsable du traitement est réputé également rempli pour toutes les communications : a. qui se fondent sur les mêmes clauses ou garanties, pour autant que les catégories de destinataires, les finalités du traitement et les catégories de données communiquées soient similaires, ou b. qui sont effectuées au sein d'une même personne morale ou société ou entre des entreprises appartenant au même groupe, aussi longtemps que les clauses ou les garanties fournies permettent d'assurer une protection appropriée des données.		
Art. 10 Clauses types de protection des données 1 Lorsqu'il communique des données personnelles à l'étranger au moyen de clauses types de protection des données au sens de l'art. 16, al. 2, let. d, LPD, le responsable du traitement prend les mesures adéquates pour s'assurer que le destinataire les respecte. 2 Le PFPDT publie une liste des clauses types de protection des données qu'il a approuvées, établies ou reconnues.	/	/
Art. 11 Règles d'entreprise contraignantes 1 Les règles d'entreprise contraignantes au sens de l'art. 16, al. 2, let. e, LPD s'appliquent à toutes les entreprises appartenant au même groupe. 2 Elles portent au moins sur les points mentionnés à l'art. 9, al. 1, ainsi que sur les points suivants : a. la structure et les coordonnées du groupe d'entreprises et de chacune de ses entités ; b. les mesures mises en place au sein des groupes d'entreprises pour garantir le contrôle du respect des règles d'entreprise contraignantes.	Al. 1 : Qu'entend-on par « groupe d'entreprises » ? Cette notion n'est pas claire quant à la structure de l'organisation et de quelle manière elle est constituée. Faut-il que les entreprises d'un groupe soient détenues à plus de 50% par les mêmes actionnaires ? Quid des succursales ?	Préciser la notion de "groupe d'entreprises".

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 12 Codes de conduite et certifications 1 Des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti par un code de conduite ou une certification. 2 Le code de conduite porte au moins sur les points mentionnés à l'art. 9, al. 1 et doit être préalablement approuvé par le PFPDT. 3 Le code de conduite ou la certification doit être assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans l'État tiers d'appliquer les mesures contenues dans ces instruments.	Al. 2 : la nLPD indique (art. 11) que "le PFPDT prend position sur les codes de conduites et publie ses prises de position". L'ordonnance va plus loin en exigeant une approbation.	Al. 2 : supprimer l'approbation du PFPDT.
Art. 13 Modalités du devoir d'informer 1 Le responsable du traitement et le sous-traitant communiquent les informations sur la collecte de données personnelles de manière concise, compréhensible et facilement accessible. 2 Lorsque l'information se fait en combinaison de pictogrammes, ceux-ci doivent être lisibles par machine s'ils sont présents par voie électronique.	Il est normalement de la responsabilité du responsable du traitement d'informer les personnes concernées (l'art. 18 nLPD ne mentionne pas le sous-traitant). La situation pouvant néanmoins se présenter en pratique, nous suggérons l'adaptation de l'al. 1 et un nouvel al. 3. Al. 2 : Dans quels contextes ces pictogrammes seraient-ils utilisés ? Aucune information dans la nLPD à ce sujet. Quels types de pictogrammes peuvent être utilisés ? Doivent-ils être reconnus par le PFPDT ?	Al. 1 : Supprimer "et le sous-traitant" Ajouter al. 3 : "Lorsque le responsable du traitement a sous-traité la collecte des données, la communication des informations échoit au sous-traitant."
Art. 14 Disposition particulière relative au devoir d'informer des organes fédéraux lors de la collecte des données personnelles Si la personne concernée n'est pas tenue de fournir des renseignements, l'organe fédéral qui collecte systématiquement des données personnelles notamment au moyen d'un questionnaire doit l'informer du caractère facultatif de sa réponse.	L'obligation d'informer figure dans la nLPD, pourquoi adopter une disposition spécifique relative aux questionnaires ?	Supprimer la disposition.
Art. 15 Informations lors de la communication des données personnelles Le responsable du traitement et le sous-traitant indiquent au destinataire l'actualité, la fiabilité et	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
l'exhaustivité des données personnelles qu'ils communiquent, dans la mesure où ces informations ne ressortent pas des données elles-mêmes ou des circonstances.		
Art. 16 Informations sur la rectification, l'effacement ou la destruction, ainsi que sur la limitation du traitement des données personnelles Le responsable du traitement informe sans délai les destinataires auxquels il a communiqué des données personnelles de la rectification, de l'effacement ou de la destruction, ainsi que de la limitation du traitement des données personnelles, sauf si la notification est impossible ou implique des efforts disproportionnés.	Les situations dans lesquelles la notification est impossible ne sont pas claires et, en outre, ne devraient jamais se produire. En outre, avec l'informatique, le cloud, les API, etc. cette notification ne devrait pas (ou très rarement) générer des efforts disproportionnés. Cette obligation nécessite de prendre des dispositions particulières en matière d'organisation et de gouvernance, un second alinéa serait pertinent à cet égard.	Supprimer "sauf si la notification est impossible ou implique des efforts disproportionnés". Ajouter un al. 2 : "Le responsable du traitement prend les mesures adéquates, notamment contractuelles et techniques, pour être en mesure de notifier les destinataires auxquels il a communiqué des données personnelles."
Art. 17 Réexamen d'une décision individuelle automatisée La personne concernée par une décision individuelle automatisée, qui demande à faire valoir son point de vue ou un réexamen de la décision par une personne physique, ne peut pas être désavantagée pour ce motif.	/	/
Art. 18 Forme et conservation de l'analyse d'impact relative à la protection des données personnelles Le responsable du traitement consigne par écrit l'analyse d'impact relative à la protection des données personnelles. Elle est conservée pendant deux ans après la fin du traitement des données.	Sur quelle base ce délai de deux ans a été défini ? De manière générale, quelles raisons ont mené à adopter des délais différents entre les articles 18 et 19 P-OLPD ? En outre, la conservation sous la forme écrite n'est pas souhaitable en regard des art. 12 et suivants CO.	Harmoniser tous les délais de conservation à 5 ans. Remplacer "par écrit" par "par tout moyen qui permet d'en apporter la preuve".
Art. 19 Annonce des violations de la sécurité des données 1 En cas de violation de la sécurité des données, le responsable du traitement annonce au PFPDT : a. la nature de la violation ; b. dans la mesure du possible, le moment et la durée ;	Al. 1 : le responsable du traitement doit être contraint dans tous les cas de fournir les informations des let. b, c et d. Il n'est pas acceptable que ces informations puissent être fournies que "dans la mesure du possible". Ces informations seront disponibles tôt ou tard dans tous les cas.	Al. 1 : Supprimer « dans la mesure du possible » aux let. b, c et d. Al. 2 : "Si le responsable du traitement n'est pas en mesure de fournir au PFPDT toutes les informations visées à l'al. 1 dans les meilleurs délais..."

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
c. dans la mesure du possible, les catégories et le nombre approximatif de données personnelles concernées ; d. dans la mesure du possible, les catégories et le nombre approximatif de per- sonnes concernées ; e. les conséquences, y compris les risques éventuels, pour les personnes concernées ; f. les mesures prises ou envisagées pour remédier à cette défaillance ou en atténuer les conséquences ; g. le nom et les coordonnées d'une personne de contact. 2 Si, lors de la détection de la violation de la sécurité des données, le responsable du traitement n'est pas en mesure de fournir au PFPDT toutes les informations visées à l'al. 1 dans le même temps, il peut les lui mettre à disposition progressivement sans retard excessif. 3 Le responsable du traitement communique à la personne concernée, dans un langage simple et compréhensible, au moins les informations visées à l'al. 1, let. a, e, f et g. 4 Lorsque le responsable du traitement est un organe fédéral, l'annonce au PFPDT est faite par l'intermédiaire du conseiller à la protection des données personnelles. 5 Le responsable du traitement documente les violations. La documentation contient tous les faits relatifs aux incidents, à leurs effets et aux mesures prises. Elle est conservée pendant au moins trois ans à compter de la date d'annonce, au sens de l'al. 1.	Al. 2 : Selon l'art. 24 al. 1 nLPD, il est indiqué que le responsable du traitement annonce dans les meilleurs délais au PFDT les violations de sécurité de données, et non lors de la détection de la violation. Al. 3 : les let. b et c devraient également être incluses, car ces informations peuvent aider les personnes concernées à déterminer l'étendue de l'incident et prendre les mesures qui s'imposent. Al. 5 : Peu clair. Quelles violations doivent être documentées ? Celles annoncées ou celles non annoncées ? Les deux ? Bien qu'il existe des doutes quant à la légalité de cet alinéa, il est utile que toutes les violations soient documentées, de manière à ce que le PFPDT ou d'autres autorités, en cas de contrôle, soient en mesure de vérifier si une violation aurait dû être annoncée alors qu'elle ne l'a pas été. Renvoi à la réflexion de l'article 18 P-OLPD pour le délai de trois ans.	Al. 5 : Le responsable du traitement documente toutes les violations. Harmoniser tous les délais de conservation à 5 ans.
Art. 20 Modalités 1 La demande de renseignement est faite par écrit. Elle peut être faite oralement moyennant l'accord du responsable du traitement. 2 Les renseignements sont en principe fournis par écrit. D'entente avec le responsable du traitement, ou sur sa proposition, la personne concernée peut également consulter ses données sur place. Si elle y a consenti,	Al. 2 : « par écrit » → même remarque que pour l'art. 18. Ici, la forme écrite ne devrait pas être érigée en principe, le responsable du traitement devrait être libre de proposer différents modes de transmission (en particulier électronique) pour autant qu'ils soient sécurisés et fiables. En outre, la personne concernée devrait pouvoir proposer de consulter les données sur	Al. 2 : supprimer la forme écrite ou y ajouter la forme électronique. Supprimer « ou sur sa proposition ». Al. 5 : "Le responsable du traitement documente le motif pour lequel il refuse, restreint ou diffère la communication des informations. La documentation est conservée pendant au moins cinq ans."

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
les renseignements peuvent également lui être fournis oralement. 3 Les renseignements fournis doivent être compréhensibles pour la personne concernée. 4 Le responsable du traitement prend les mesures adéquates pour assurer l'identification de la personne concernée et pour protéger les données de la personne concernée de tout accès de tiers non autorisé lors de la communication des renseignements. La personne concernée est tenue de collaborer à son identification. 5 Le responsable du traitement documente le motif pour lequel il refuse, restreint ou diffère la communication des informations. La documentation est conservée pendant au moins trois ans.	place, cette prérogative ne devrait pas appartenir uniquement au responsable du traitement. Al. 5 : La durée de 3 ans est trop courte. Prévoir au moins 5 ans (cf. supra). La terminologie utilisée (informations, renseignements) prête à confusion. Parle-t-on des mêmes données ? Il serait opportun d'uniformiser la terminologie.	Uniformiser la terminologie.
Art. 21 Responsabilité 1 Lorsqu'il existe plusieurs responsables pour le traitement des données personnelles, la personne concernée peut exercer son droit d'accès auprès de chacun d'eux. Si l'un des responsables du traitement n'est pas compétent pour traiter la demande, il la transmet au responsable du traitement compétent. 2 Si la demande de renseignement porte sur des données traitées par un sous-traitant, le responsable du traitement transmet la demande au sous-traitant s'il n'est pas en mesure de fournir les renseignements lui-même.	Il est regrettable qu'aucune disposition ne règle la question générale des responsabilités entre responsables conjoints du traitement à l'instar de l'art. 26 RGPD.	Al. 1 : "il la transmet sans délai..."
Art. 22 Délais 1 Les renseignements sont fournis dans les 30 jours suivant réception de la demande. Si le responsable du traitement refuse, restreint ou diffère le droit d'accès, il le communique dans le même délai. 2 Si les renseignements ne peuvent être donnés dans les 30 jours, le responsable du traitement en avertit la personne concernée en lui indiquant le délai dans lequel les renseignements seront fournis.	Al. 2 : selon l'art. 25 al. 7 nLPD, en règle générale, les renseignements sont fournis dans un délai de 30 jours (suivant réception de la requête). Il doit en être de même pour toutes les situations qu'il s'agisse d'une demande de renseignements ou d'un refus d'accès.	Al. 2 : "Si les renseignements, ou si la décision relative au refus, à la restriction ou au report du droit d'accès, ne peuvent être donnés dans les 30 jours, le responsable du traitement en avertit la personne concernée en lui indiquant le délai dans lequel ceux-ci seront fournis."

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 23 Exceptions à la gratuité 1 Une participation équitable aux frais peut être demandée lorsque la communication des renseignements occasionne des efforts disproportionnés. 2 Le montant prélevé s'élève à 300 francs au maximum. 3 La personne concernée est préalablement informée du montant et peut retirer sa requête dans les dix jours.	Al. 3 : Est-ce que ce délai de 10 jours suspend le délai global de 30 jours de l'art. 25 al. 7 nLPD et de l'art. 22 P-OLPD ? En effet, le responsable du traitement peut mettre quelques jours à déterminer si la requête sort du principe de la gratuité et, ce faisant, « travaille » déjà à y répondre. Bien qu'il soit contraire au principe du droit d'accès d'exiger le paiement de frais, il serait bienvenu (pour la sécurité du droit et la pratique) d'indiquer qu'en l'absence de réponse, et après un rappel, la personne concernée est réputée avoir retiré sa requête.	Al. 3 : "La personne concernée est préalablement informée du montant et peut retirer sa requête dans les dix jours. La requête est réputée retirée dans le cas où, après un rappel, le montant demandé n'est pas payé dans le second délai de 10 jours." Préciser aussi si le délai de 10 jours suspend le délai de 30 jours.
Art. 24 Les art. 20 al. 1, 4 et 5, ainsi que 21, 22 et 23 s'appliquent par analogie à la remise et à la transmission des données personnelles, ainsi qu'à leurs éventuelles restrictions.	/	/
Art. 25 Conseiller à la protection des données 1 Le conseiller à la protection des données personnelles d'un responsable du traitement privé doit accomplir les tâches suivantes : a. contrôler le traitement de données personnelles ainsi que ses exigences et proposer des mesures s'il constate que des prescriptions de protection des données ont été violées ; b. concourir à l'établissement de l'analyse d'impact relative à la protection des données, et la vérifier, dans tous les cas lorsque le responsable du traitement privé entend renoncer à consulter le PFPDT au sens de l'art. 23, al. 4, LPD ; 2 Le responsable du traitement privé : a. met à disposition du conseiller à la protection des données personnelles les ressources nécessaires ; b. donne au conseiller à la protection des données accès à tous les renseignements, documents, registres des activités de traitement et données personnelles dont il a besoin pour l'accomplissement de ses tâches.	Ces précisions sont bienvenues, mais la nLPD laisse-t-elle la possibilité au Conseil fédéral de compléter ainsi la loi sur des aspects impliquant les personnes privées ? L'art. 10 al. 4 nLPD ne mentionne que les organes fédéraux. La base légale semble (malheureusement) manquante.	A regret : supprimer l'art. 25. Si la disposition est maintenue : • Décrire plus précisément les tâches du conseiller (p. ex. sous la forme d'un inventaire ou d'une description de fonction) • Rapprocher le plus possible la fonction de conseiller d'un responsable du traitement privé de la fonction de conseiller d'un organe fédéral (cf. art. 29) • Préciser quelle est la responsabilité (civile, pénale) du conseiller

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 26 Exception à l'obligation de tenir un registre des activités de traitement Les entreprises et autres organismes de droit privé employant moins de 250 collaborateurs au début d'une année, ainsi que les personnes physiques, sont déliés de leur obligation de tenir un registre des activités de traitement, à moins que l'une des conditions suivantes soit remplie : a. le traitement porte sur des données sensibles à grande échelle ; b. le traitement constitue un profilage à risque élevé.	C'est cohérent avec l'art. 22 al. 2 nLPD mais problématique. Le simple fait de traiter des données sensibles, de réaliser des profilages, d'utiliser des techniques de machine learning et de traiter de grandes quantités de données (même non sensibles) etc. est susceptible de créer un risque important pour les personnes concernées. Les exceptions listées sous lettres a et b sont trop larges et s'appliqueront à un grand nombre d'entreprises, ce qui vide de son sens et de son utilité la tenue d'un registre de traitement. La création et la tenue d'un registre, même sous une forme simple pour une PME, sont un exercice indispensable à une bonne gouvernance de la protection et de la sécurité des données. Pousser les entreprises à documenter leurs traitements et les mesures de sécurité associées va dans le sens d'une meilleure responsabilisation des entreprises et protection des personnes concernées. Le rapport explicatif de l'OLPD ne s'y trompe pas puisqu'il affirme que le registre des traitements est un instrument simple et efficace. En outre, le registre des activités de traitement constitue la base pour un programme de protection des données et la prise de mesures de sécurité adéquates.	Prévoir des conditions plus nombreuses, mais moins larges. S'inspirer de l'art. 30 al. 5 RGPD. Le traitement de données sensibles devrait systématiquement conduire à l'établissement d'un registre des traitements, de même que tout traitement constituant un profilage.
Art. 27 Désignation Tout organe fédéral désigne un conseiller à la protection des données personnelles. Plusieurs organes fédéraux peuvent désigner conjointement un conseiller.	/	/
Art. 28 Exigences et tâches 1 Le conseiller à la protection des données personnelles doit remplir les conditions suivantes : a. il dispose des connaissances professionnelles nécessaires ;	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
b. il exerce sa fonction de manière indépendante par rapport à l'organe fédéral et sans recevoir d'instruction de celui-ci. 2 Il accomplit les tâches suivantes : a. contrôler le traitement de données personnelles ainsi que ses exigences et proposer des mesures s'il constate que des prescriptions de protection des données ont été violées ; b. concourir à l'établissement de l'analyse d'impact relative à la protection des données et la vérifier ; c. annoncer au PFPDT les violations de la sécurité des données ; d. servir de point de contact pour les personnes concernées ; f. former et conseiller l'organe fédéral et ses collaborateurs en matière de protection des données.		
Art. 29 Devoirs de l'organe fédéral 1 L'organe fédéral donne au conseiller à la protection des données accès à tous les renseignements, documents, registres des activités de traitement et données personnelles dont il a besoin pour l'accomplissement de ses tâches. 2 Il publie les coordonnées du conseiller à la protection des données personnelles en ligne et les communique au PFPDT.	/	/
Art. 30 Interlocuteur du PFPDT Le conseiller à la protection des données personnelles est l'interlocuteur du PFPDT fédéral pour les questions relatives au traitement des données personnelles par l'organe concerné.	/	/
Art. 31 Information du conseiller à la protection des données L'organe fédéral responsable informe le conseiller à la protection des données en temps utile lors de la conception d'un projet de traitement automatisé de données personnelles, ainsi qu'en cas de modifications après l'achèvement du projet, afin que les exigences de	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
la protection des données soient prises en compte à temps.		
Art. 32 Annonce au PFPDT 1 L'organe fédéral responsable informe le PFPDT des activités prévues de traitement automatisé au moment de l'approbation du projet ou de la décision de le développer. Le PFPDT enregistre cette information dans le registre des activités de traitement. 2 L'annonce contient les informations prévues à l'art. 12, al. 2, let. a à d LPD, ainsi que la date prévue pour le début des activités de traitement. 3 L'organe fédéral responsable actualise cette annonce lors du passage à la phase de production ou lorsque le projet est abandonné.	/	/
Art. 33 Caractère indispensable de la phase d'essai Une phase d'essai, en tant qu'essai pilote, peut être considérée comme indispensable si l'une des conditions suivantes est remplie : a. l'accomplissement des tâches nécessite l'introduction d'innovations techniques dont les effets doivent être évalués ; b. l'accomplissement des tâches nécessite la prise de mesures organisationnelles ou techniques importantes dont l'efficacité doit être examinée, notamment dans le cadre d'une collaboration entre les organes fédéraux et les cantons ; c. l'accomplissement des tâches nécessite de rendre accessibles en ligne les données personnelles faisant l'objet d'un traitement.	/	/
Art. 34 Autorisation 1 Avant de consulter les unités administratives concernées, l'organe fédéral responsable de l'essai pilote communique au PFPDT de quelle manière il est prévu d'assurer que les exigences de l'art. 35 LPD sont remplies et l'invite à prendre position. 2 Le PFPDT prend position sur le respect des exigences de l'art. 35 LPD. A cet effet, l'organe fédéral	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
responsable lui remet tous les documents nécessaires et en particulier : a. un descriptif général de l'essai pilote ; b. un rapport démontrant que l'accomplissement des tâches légales nécessite le traitement au sens de l'art. 34, al. 2, LPD et rend indispensable une phase d'essai avant l'entrée en vigueur de la loi au sens formel (art. 35, al. 1, let. c, LPD) ; c. un descriptif de l'organisation interne et des processus de traitement et de contrôle des données ; d. un descriptif des mesures de sécurité et de protection des données ; e. un projet d'ordonnance réglant les modalités de traitement ou les grandes lignes de cet acte législatif ; f. les informations concernant la planification des différentes phases de l'essai pilote. 3 Le PFPDT peut exiger d'autres documents et procéder à des vérifications complémentaires. 4 L'organe fédéral responsable informe le PFPDT de toute modification essentielle portant sur le respect des conditions de l'art. 35 LPD. Le cas échéant, le PFPDT prend à nouveau position. 5 La prise de position du PFPDT est annexée à la proposition adressée au Conseil fédéral. 6 Les modalités du traitement automatisé sont réglées par voie d'ordonnance.		
Art. 35 Rapport d'évaluation L'organe fédéral responsable soumet pour avis au PFPDT le projet de rapport portée à la connaissance du Conseil fédéral.	/	/
Art. 36 Lorsque des données personnelles sont traitées à des fins ne se rapportant pas à des personnes, en particulier en cas de recherche, de planification ou de statistique, et que le traitement sert également une autre finalité, les dérogations prévues à rapportant pas à des personnes.	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 37 Siège et secrétariat permanent 1 Le siège du PFPDT est à Berne. 2 Les rapports de travail du personnel du secrétariat permanent du PFPDT sont régis par la législation fédérale sur le personnel. Le personnel du secrétariat permanent du PFPDT est assuré auprès de la Caisse de pensions PUBLICA, à savoir la Caisse de prévoyance de la Confédération, contre les conséquences économiques de la vieillesse, de l'invalidité et du décès.	/	/
Art. 38 Moyen de communication 1 Le PFPDT communique avec le Conseil fédéral par l'intermédiaire du Chancelier de la Confédération. Celui-ci transmet les propositions, prises de positions et rapports au Conseil fédéral sans les modifier. 2 Le PFPDT transmet les rapports destinés à l'Assemblée fédérale par l'intermédiaire des Services du Parlement.	/	/
Art. 39 Communication des directives et des décisions 1 Les départements et la Chancellerie fédérale communiquent au PFPDT leurs directives en matière de protection des données, ainsi que leurs décisions sous forme anonyme. 2 Les organes fédéraux communiquent au PFPDT tous leurs projets législatifs concernant la protection des données personnelles et l'accès aux documents officiels.	/	/
Art. 40 Traitement des données Le PFPDT traite les données personnelles, y compris les données sensibles, notamment aux fins suivantes : a. exercer ses activités de surveillance ; b. enquêter sur les violations des règles de protection des données ; c. former et conseiller des organes fédéraux et des personnes privées ; d. collaborer avec les autorités cantonales, fédérales et étrangères ;	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
e. mettre en œuvre des procédures de conciliation et des évaluations au sens de la loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (LTrans) ; f. répondre aux questions des citoyens.		
Art. 41 Autocontrôle 1 Le PFPDT établit un règlement pour tous les traitements automatisés. L'art. 5, al. 1 ne s'applique pas. 2 Il prévoit des processus internes afin de garantir que le traitement des données soit effectué conformément au règlement de traitement. Il vérifie annuellement le respect du règlement de traitement.	/	/
Art. 42 Collaboration avec le Centre national pour la cybersécurité (NCSC) 1 Le PFPDT peut transmettre les informations relatives à l'annonce d'une violation de la sécurité des données au NCSC afin qu'il analyse l'incident. Le PFPDT doit au préalable obtenir l'accord de la personne responsable de l'annonce. 2 Il invite le NCSC à se prononcer avant d'ordonner une mesure au sens de l'art. 51, al. 3, let. b, LPD à l'encontre de l'organe fédéral concernant la sécurité des données.	/	/
Art. 43 Registre des activités de traitement des organes fédéraux 1 Le registre des activités de traitement des organes fédéraux contient les informations fournies par les organes fédéraux et leurs sous-traitants conformément à l'art. 12, al. 2 et 3, LPD, ainsi qu'à l'art. 32, al. 2, de la présente ordonnance. 2 Il est publié en ligne. Les inscriptions au registre concernant les activités prévues de traitement automatisé, au sens de l'art. 32, ne sont pas publiées.	/	/
Art. 44 Codes de conduite	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Si un code de conduite est soumis au PFPDT, celui-ci indique dans sa prise de position si le code de conduite remplit les conditions de l'art. 22, al. 5, let. a et b, LPD.		
Art. 45 Emolument 1 L'émolument perçu par le PFPDT se calcule en fonction du temps consacré. 2 Il varie entre 150 et 350 francs l'heure. Il dépend de la complexité de l'affaire et de la fonction de la personne chargée de la traiter. 3 L'ordonnance générale sur les émoluments du 8 septembre 2004s'applique pour le surplus.	/	/
Art. 46 Abrogation et modification d'autres actes L'abrogation est la modification d'autres actes sont réglés à l'annexe 2.	/	/
Art. 47 Disposition transitoire concernant l'annonce au PFPDT des activités prévues de traitement automatisé L'art. 32 ne s'applique pas aux activités prévues de traitement automatisé pour lesquelles l'approbation du projet ou la décision de le développer a déjà été prise au moment de l'entrée en vigueur de la présente ordonnance.	/	/
Art. 48 Entrée en vigueur La présente ordonnance entre en vigueur le ...	/	/

L'ASDPO souhaite remercier vivement Mesdames Laura Menétrey, Nesrin Keles, Isabelle Hering, Anne-Sylvie Aubert, Laura Bares et Mounira Fellag, ainsi que Messieurs Lauris Loat, Stéphane Droxler et François Charlet pour leurs contributions éclairées à cette prise de position.

Schweizerischer Pensionskassenverband
Association suisse des Institutions de prévoyance
Associazione svizzera delle Istituzioni di previdenza
Kreuzstrasse 26
8008 Zürich

Telefon 043 243 74 15/16
Telefax 043 243 74 17
E-Mail info@asip.ch
Website www.asip.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
jonas.amstutz@bj.admin.ch

3003 Bern

Zürich, 8. Oktober 2021

Stellungnahme zur Vernehmlassung betreffend den Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren,

Gerne nehmen wir zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellung.

Grundsätzlich enthält die obligatorische berufliche Vorsorge (BVG) eine in sich geschlossene Datenschutzkonzeption, so dass diese Bestimmungen jenen des allgemeinen DSG grundsätzlich vorgehen («lex specialis»). Gleichwohl gelten die registrierten Vorsorgeeinrichtungen für den obligatorischen Bereich der beruflichen Vorsorge als Bundesorgane (Art. 5 lit. i revDSG) gemäss Art. 2 Abs. 1 lit. b revDSG, im Bereich der überobligatorischen beruflichen Vorsorge (umhüllende Vorsorge) gelten sie hingegen als private Personen gemäss Art. 2 Abs. 1 lit. a revDSG, was auch für die nicht registrierten Vorsorgeeinrichtungen (ausserobligatorische berufliche Vorsorge) gilt (Art. 2 Abs. 1 lit.a revDSG).

Soweit allerdings nicht eine abschliessende spezialgesetzliche Norm vorliegt, müssen die registrierten Vorsorgeeinrichtungen immer auch die allgemeinen Bestimmungen des DSG beachten. Schliesslich sind die Grundsätze des DSG auch bei der Auslegung bereichsspezifischer Normen zu berücksichtigen (A-4467/2011 vom 10. April 2012).

Im Unterschied zu den Archivierungsvorschriften von Art. 41 Abs. 8 BVG i.V.m. Art. 27j BVV 2, die auch im überobligatorischen (umhüllenden) Bereich (Art. 49 Abs. 2 Ziff. 6 BVG) und im ausserobligatorischen Bereich (Art. 89a Abs. 6 Ziff. 5 ZGB) der beruflichen Vorsorge mit reglementarischen Leistungen zur Anwendung kommen, gelten – mit Ausnahme von Art. 85a lit. f BVG und Art. 86a Abs. 2 lit. b^{bis} BVG – die datenschutzrechtlichen Bestimmungen des BVG jedoch nicht in der weitergehenden und ausserobligatorischen beruflichen Vorsorge (vgl. Art. 49 Abs. 2 Ziff. 25a und 25b BVG; Art. 89a Abs. 6 Ziff. 5a, Abs. 7 Ziff. 2 ZGB), in welcher lediglich die Bestimmungen des DSG zur Anwendung kommen.

Da der von uns in der Vernehmlassungsantwort vom 4. April 2017 eingebrachte Antrag, für die über- und ausserobligatorische Vorsorge, d.h. für registrierte Vorsorgeeinrichtungen mit umhüllender Vorsorge und nicht registrierte Vorsorgeeinrichtungen mit reglementarischen Leistungen bzw. mit Ermessensleistungen, den Verweis auf Art. 85a BVG in Art. 49 Abs. 2 BVG bzw. Art. 89a Abs. 6 und 7 ZGB aufzunehmen, abgelehnt worden war, beantragen wir, in Art. 7 revVDSG eine präzisierende Ergänzung anzubringen, da in diesem Kontext mit «Bundesorgan» nicht die registrierten Vorsorgeeinrichtungen gemeint sein können, bei denen es sich zwar um Bundesorgane gemäss Art. 2 Abs. 1 lit. b i.V.m. Art. 5 lit. i revDSG handelt, jedoch in der Eigenschaft von Auftragsbearbeitern i.S. von Art. 5 lit. k revDSG.
Als Präzisierung schlagen wir deshalb vor: «Nicht gemeint sind Bundesorgane als Auftragsbearbeiter gemäss Art. 2 Abs. 1 lit. b i.V.m. Art. 5 lit. i revDSG.»

Im Weiteren beantragen wir die Streichung von Art. 19 Abs. 4 revVDSG, der für Bundesorgane die Meldung von Verletzungen der Datensicherheit an den EDÖB über die Datenschutzberaterin oder den Datenschutzberater gemäss Art. 10 revDSG verlangt. Müssten nämlich sämtliche registrierten Vorsorgeeinrichtungen, die ja als Bundesorgane i.S. des revDSG gelten, «durch Weisungen oder andere geeignete Instrumente» sicherstellen, «dass die verantwortlichen Fachbereiche die Datenschutzberaterin oder den Datenschutzberater unverzüglich über Verletzungen der Datensicherheit informieren, damit diese oder dieser die Meldung gemäss Artikel 24 Abs. 1 nDSG so rasch als möglich vornehmen kann» (Erläuternder Bericht zur Revision der Verordnung zum Bundesgesetz über den Datenschutz, S. 33), so würde dies deren Verwaltungskosten immens in die Höhe treiben. Dadurch würde die Durchführung der obligatorischen beruflichen Vorsorge, die ja bereits an einem viel zu hohen Umwandlungssatz (6,8%) leidet, weiter erschwert.

Gleichzeitig ersuchen wir Sie, Art. 27 revVDSG, der von jedem Bundesorgan verlangt, eine Datenschutzberaterin oder einen Datenschutzberater zu ernennen, mit folgendem Zusatz zu versehen: «Ausgenommen sind die gemäss BVV 1 registrierten Vorsorgeeinrichtungen.»

Aufgrund der Komplexität der Materie schlagen wir zudem vor, das revDSG und die revVDSG frühestens auf den 1. Januar 2023 in Kraft treten zu lassen (keine unterjährige Inkraftsetzung).

Wir danken Ihnen für die Berücksichtigung unserer Hinweise.

Mit freundlichen Grüssen

A S I P

Schweizerischer Pensionskassenverband

Jean Rémy Roulet

Präsident

Hanspeter Konrad

Direktor

Herr
Jonas Amstutz
Eidgenössisches Justiz-
und Polizeidepartement EJPD
Bundesrain 20
3003 Bern

Ausschliesslich per E-Mail an:
jonas.amstutz@bj.admin.ch

Bern, 11. Oktober 2021

Stellungnahme ASPS zur Revision der Verordnung über den Datenschutz (VDSG)

Sehr geehrter Herr Amstutz, sehr geehrte Damen und Herren

Die Association Spitex privée Suisse ASPS ist der nationale Verband der privaten Spitex-Anbietenden. Sie vertritt schweizweit über 300 Spitex-Organisationen mit über 13‘000 Mitarbeitenden. Die ASPS unterstützt Initiativen, die Transparenz in der Finanzierung von Spitex-Dienstleistungen ermöglichen. Klare Strukturen in den Kosten- und Subventionsflüssen sind anzustreben, damit wegweisende Lösungen möglich werden.

Die Rahmenbedingungen privater Engagements sind generell zu verbessern, um dem steigenden Spitex-Bedarf zuhause, in Alterssiedlungen und bei den Formen des Betreuten Wohnens gerecht zu werden.

Organisationen, welche im Gesundheitswesen tätig sind, bearbeiten höchstpersönliche und heikle Daten, deren Bekanntgabe ein hohes Risiko für die Persönlichkeit der Leistungsbeziehenden aufweisen können. Es ist angemessen, diese Daten zu schützen. Da unsere Mitglied-Organisationen direkt betroffen sind, erlauben wir uns hiermit, im Namen unserer Mitglieder zur vorgelegten Revision der Verordnung über den Datenschutz (VDSG) Stellung zu nehmen.

Wir sind darauf bedacht, dass die vom Bundesrat vorgeschlagenen Umsetzungsmodalitäten möglichst schlank, praxisnah für die Organisationen und anwendungsfreundlich ausfallen.

Bei den parlamentarischen Beratungen zum revidierten Datenschutzgesetz (DGS) standen die Eingliederung der internationalen Entwicklungen und die Vermeidung von Schweizer Besonderheiten im Zentrum.

Die vorliegende Revision der Verordnung erfüllt weder unser Anliegen einer praxisnahmen und anwendungsfreundlichen Umsetzung, noch folgt sie den Prinzipien des Parlaments bei der Entstehung des revidierten DSG. Die VDSG strebt offensichtlich eine sehr genaue und umfangreiche Einhaltung des Datenschutzes an. Der Entwurf der VDSG wirkt wie ein unabhängig des revidierten DSG entstandenes Regelwerk.

Association Spitex privée Suisse ASPS | Uferweg 15 | 3000 Bern 13
Tel 031 370 76 73 | Fax 031 370 76 77 | info@spitexprivee.swiss | www.spitexprivee.swiss

Gestützt darauf beantragen wir den vorliegenden Verordnungsrevision so zu überarbeiten, dass die Verordnung **kohärent zum DSG** wird.

Besonders wichtig darin ist der ASPS:

- eine Ergänzung in Art. 20, Abs. 3 «… soweit dies im Rahmen des kognitiven Zustands möglich ist.»

  Verständlichkeit bedeutet nicht, dass der Verantwortliche der um Auskunft ersuchenden Person die Datensätze oder darüber hinaus gehend sogar die damit einhergehenden Abläufe und Geschäftsmodelle erklären muss. Will die auskunftsberechtigte Person mehr über solche über den eigentlichen Herausgabeanspruch hinaus gehende Verhältnisse erfahren, muss sie sich an einen Rechtsanwalt oder Wirtschaftsfachmann halten, nicht an den Verantwortlichen.

- Betreffend Art. 26 Abs. 1 (Lit. a. und b.) wünschen wir uns eine klare Abgrenzung für die Ausnahmefälle (Was heisst «umfangreich besonders schützenswerte Personendaten»? Was ist «hohes Risiko») => Wenn hier keine (messbaren) Präzisierungen gemacht werden, wird es gerade in unseren Organisationen grosse Rechtsunsicherheiten geben.

- Bei Artikel 45 ist uns wichtig, dass im Sinne einer rechtmässigen Umsetzung der komplexen neuen Datenschutzgesetzgebung das Anrufen des EDÖB nicht durch das Erheben von Gebühren entgegengewirkt wird.

Im Anhang finden Sie Details zu unserem Antrag.

Besten Dank für die Berücksichtigung unserer Anliegen. Für Fragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Association Spitex privée Suisse ASPS

Marcel Durst
Geschäftsführer

Kai-Bernhard Trachsel
Stv. Geschäftsführer

Association Spitex privée Suisse ASPS | Uferweg 15 | 3000 Bern 13
Tel 031 370 76 73 | Fax 031 370 76 77 | info@spitexprivee.swiss | www.spitexprivee.swiss

Anhang: Details zum Antrag ASPS

Zur Kohärenz zum DSG beantragen wir, dass in der VDSG etwas stumpfe Begriffe und Abgrenzungen im Sinne einer möglichst klaren und praxisnahmen Umsetzungshilfe präziser umschrieben werden.

Des Weiteren beantragen wir eine möglichst konkrete, zugängliche und auch finanziell günstige Unterstützung der Betriebe durch die zuständigen staatlichen Stellen – v.a. durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Namentlich sind folgende Verordnungsänderungen für die Organisationen im Gesundheitswesen relevant:

- die Bestimmungen über die Mindestanforderungen an die Datensicherheit
- die Modalitäten der Informationspflichten und des Auskunftsrechts
- die Meldung von Verletzungen der Datensicherheit
- die Ausnahmen, in welchen persönliche Verantwortliche mit weniger als 250 Mitarbeitenden von der Pflicht befreit sind, ein Verzeichnis der Bearbeitungstätigkeiten zu führen.
- für die Bekanntgabe von Personendaten ins Ausland: die Kriterien, gemäss welchen der Bundesrat beurteilt, ob er das Datenschutzrecht eines Staates als angemessen erachtet oder nicht

E-VDSG	**Kommentar**	**Antrag / Neuformulierung**
Art. 1 Abs. 1	Die vorgeschlagene Umschreibung ist im Grundsatz zu begrüssen. Sie ergänzt und konkretisiert sinnvollerweise Artikel 8 Absatz 1 nDSG. Zu begrüssen ist, dass sie möglichst schlank und angesichts der stetigen technischen Entwicklungen flexibel, praxisnah und anwendungsfreundlich gehalten worden ist. Weil sie sehr allgemein formuliert ist, braucht es aber entsprechende Deutungs- und Umsetzungshilfen für die Praxis.	- Es müssen seitens EDÖB möglichst bald Dokumente geschaffen werden, welche den Betrieben die Praxisumsetzung vereinfachen.
Art. 1 Abs. 2	Die Abstände zwischen den vorzunehmen Überprüfungen sollten präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Was genau „angemessene Abstände“ sind, hängt selbstverständlich von den Besonderheiten des konkreten Anwendungsfalls ab (S. 17 im erläuternden Bericht: «[…] bei der Bestimmung der Massnahmen selbstredend die Umstände des Einzelfalls massgeblich [bleiben]»). Während die Datenbearbeiter inhaltlich grossen Freiraum für die Bestimmung ihrer konkreten Massnahmen brauchen, sollte zeitlich zumindest eine konkrete Anforderung gelten, um die Sicherheit zu gewährleisten. Als sinnvoll erscheint uns eine mindestens jährliche Überprüfung.	[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen, jedoch mindestens einmal pro Jahr zu überprüfen.

Art. 2	Diese präzise Auflistung der Schutzziele macht Sinn: Sie stellt eine praxisorientierte ‚Gedächtnisstütze' für die Verantwortlichen und die Auftragsbearbeiter dar, was im Rahmen ihrer Konkretisierung zu berücksichtigen ist. Wichtig ist eine gute Anwendbarkeit in der Praxis (Seite 17 des Berichts: „In Anwendung der Verhältnismässigkeit sind ausgehend […] von dieser Auflistung der Schutzziele] die organisatorischen und technischen Massnahmen des Einzelfalls zu bestimmen.") Gleichzeitig zeigt diese Auflistung die Komplexität der Anforderungen an eine gesetzkonforme Datenbearbeitung und -sicherheit auf; mit dem damit verbundenen Aufwand. Aus diesem Grund ist eine möglichst konkrete und für Schweizer Betriebe auch unentgeltliche Unterstützung der Datenschutzverantwortlichen durch die zuständigen Behörden (insbesondere das EDÖB), vorzusehen. So können die Umsetzungskosten durch Wirtschaft und Gesellschaft minimiert und angemessene Datensicherheit auf allen Ebenen geschaffen werden.	- Für eine optimale und kostengünstige Umsetzung ist darauf zu achten, dass Schweizer Unternehmen einen guten und kostengünstigen Zugang zum EDÖB erhalten (vgl. auch Art. 45 Abs. 2).
Art. 3	Welche „Massnahmen" im vorliegenden Rahmen berücksichtigt werden sollen und ob ein Risiko als hoch oder begrenzt beurteilt werden soll, dürfte in der Praxis oftmals schwierig zu beurteilen sein, denn Artikel 8 nDSG führt auch keine präziseren Anhaltspunkte über die Art der infrage stehenden Massnahmen. Dies entspricht zwar einer flexiblen, bedarfsorientierten und dem neusten technischen Stand angepassten Umsetzung des Datenschutzes, macht aber dessen Realisierung in der Praxis schwierig. In diesem Sinne ist die Präzisierung der Inhalte der Protokollierung (gemäss Abs. 3) an sich konsequent und kongruent. Sie weist aber einen hohen Detaillierungsgrad auf, der einen entsprechend hohen Umsetzungsaufwand, eine Unübersichtlichkeit und mögliche Verwechslungsrisiken mit sich bringt. Es ist festzustellen, dass gerade bei der *automatisierten* Bearbeitung von Personendaten die Anforderung einer detaillierten Protokollierung einen beträchtlichen Teil der Vorteile der Automatisierung beraubt: Der zeitliche und administrative Aufwand wird erheblich vergrössert. *Antrag:* Es sollen Alternativen zur Protokollierung als Massnahmen zum Datenschutz im E-VDSG vorgesehen werden – wie etwa die physische/räumliche Sicherung der Daten,	In Art. 3 Abs. 1 müssen Alternativen zur im Entwurf vorgesehenen (komplexen) Protokollierung – vorgesehen werden, namentlich etwa Zugriffskontrollen, die physische/räumliche Sicherung der Daten, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.

	Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.	
Art. 4 Abs. 2	Weil in sehr vielen Fällen eine automatisierte Bearbeitung von besonders schützenswerten Personendaten erfolgt, sind die von dieser Bestimmung gestellten Anforderungen als zu aufwendig und vielfach unnötig zu qualifizieren. Sie bringen für die betroffenen Datenbearbeiter unangemessen hohe Kosten mit sich. Deswegen ist diese Auflistung zu kürzen: Die Buchstaben d, e und j sollen ersatzlos gestrichen werden, weil sie unnötige zusätzliche Anforderungen und Präzisierungen darstellen, die den administrativen Aufwand für die Betriebe verschärfen, ohne dass daraus ein entsprechender Nutzen entsteht. Buchstabe i soll gekürzt werden: Er weist einen Detaillierungsrad mit entsprechenden Umsetzungskosten auf, der in keinem vernünftigen Verhältnis zu seinem realen Nutzen steht. Hingegen werden Buchstaben f und g ausdrücklich begrüsst, da sie zentrale Massnahmen zur Gewährleistung der Datensicherheit darstellen. Ihre Einhaltung genügt, um dem Datenschutz gerecht zu werden. Auch Buchstabe h wird begrüsst, weil eine stets angestrebte Datenminimierung das beste Mittel darstellt, um sowohl den Schutz der Privatsphäre als auch die Verminderung des mit jeglichem Datenbearbeitung verbundenen administrativen Aufwands zu erreichen.	[2] Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. ~~zur internen Organisation~~; e. ~~zur Herkunft der Personendaten und zur Art ihrer Beschaffung~~; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den ~~Datenbearbeitungsverfahren, insbesondere den~~ Verfahren bei der Speicherung, ~~Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung,~~ Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. ~~zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf~~

		~~Datenherausgabe oder -übertragung.~~
Art. 4 Abs. 3	Wie gemäss obigem Antrag in Art. 1 Abs. 2 sollten auch hier die zeitlichen Abstände zwischen den vorzunehmen Aktualisierungen präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Deswegen wird hier beantragt, dass die Aktualisierungen mindestens einmal jährlichen stattfinden.	[3] Die private Person muss das Reglement ~~regelmässig~~ in angemessenen Abständen, jedoch mindestens einmal pro Jahr, aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.
Art. 6 Abs. 2	Die in dieser Bestimmung gestellten Anforderungen an die nicht dem DSG unterstellten Datenbearbeiter sind offensichtlich zu hoch. Von einer nicht unterstellten Instanz kann nicht verlangt werden, dass sie Kenntnis der vielen potenziell relevanten Gesetzesbestimmungen und der möglichen Abhilfe-Lösungen haben. Wennschon ist es die Pflicht von Gesetzgeber und Verwaltung, den Datenschutz so auszugestalten, dass er – wo nötig und sinnvoll – überall für alle Betroffenen gleichermassen gilt. Diese Pflicht den einzelnen Verantwortlichen aufzubürden, wie der Bundesrat es vorschlägt, führt zu enormer Unsicherheit und Aufwand. Deswegen ist dieser Absatz ersatzlos zu streichen.	[2] ~~Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen~~ ~~Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege~~ ~~sicherstellen.~~
Art. 8 Abs. 1	Weder aus der Formulierung dieser Bestimmung noch aus dem erläuternden Bericht geht klar hervor, wer für die Beurteilung der Angemessenheit des Datenschutzes in einem anderen Staat zuständig ist. Aus dem erläuternden Bericht hingegen schon (S. 25 ff): Der Bundesrat. Der Klarheit halber sollte diese Zuständigkeit in Art. 8 E-VDSC klar geregelt werden, sonst besteht das Risiko, dass sich private Akteure dafür verantwortlich halten – was ihre Kapazitäten sprengen würde.	[1] Werden Personendaten ins Ausland bekanntgegeben, so müssen ~~bei der~~ anlässlich einer regelmässigen Beurteilung durch den Bundesrat, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden: […]
Art. 8 Abs. 3	Die Abstände zwischen den vorzunehmen Beurteilungen sollen präziser angegeben werden. Deswegen wird auch	[3] Die Angemessenheit des Datenschutzes des

	hier beantragt, dass die Beurteilungen mindestens einmal jährlich stattfinden müssen.	betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch, jedoch mindestens einmal pro Jahr, neu beurteilt.
Art. 9 Abs. 1	Die von Art. 9 E-VDSG gestellten Anforderungen erreichen ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Zwar sind diese Anforderungen für das Ziel des Datenschutzes konsequent, sie verursachen aber hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden. Namentlich Bst. h ist klarerweise unnötig; seine Anwendung wäre unverhältnismässig aufwendig. Andere bestehende Bestimmungen genügen, um die Garantien zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.	[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen die Datensicherheit mindestens die folgenden Punkte regeln: […] h. ~~die Massnahmen zur Gewährleistung der Datensicherheit;~~ […]
Art. 10	Wir begrüssen, dass der EDÖB eine Liste von Standard-Datenschutzklauseln veröffentlicht, um den Aufwand für die Betroffenen zu reduzieren und eine gewisse Vereinheitlichung der Schutzklauseln zu erreichen.	-
Art. 15	Bei der Anwendung dieser Bestimmung ist darauf zu achten, dass die Anforderungen der mit der Bekanntgabe von Personendaten verbundenen Informationen nicht zu umfangreich ausfallen müssen. Meistens werden sich die zum Datenschutz nötigen Informationen aus den Daten oder den Begleitumständen selbst ergeben.	-
Art. 18	Nach unserer Einschätzung reicht es aus, wenn *nach Beendigung der Datenbearbeitung* (was bei entsprechenden Gerichtsverfahren bereits Jahre dauern kann) eine Aufbewahrung für ein Jahr statt zwei Jahre stattfindet.	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während ~~zwei Jahren~~ einem Jahr nach Beendigung der Datenbearbeitung aufbewahrt werden.

Art. 20	Die vorgesehene Dreifachlösung (schriftlich, mündlich oder durch Einsichtnahme an Ort und Stelle) erscheint als sehr sinnvoll. So kann für Menschen mit gewissen Krankheiten oder Beeinträchtigungen eine geeignete Lösung gefunden werden. Für gewisse Fälle, wie urteilsunfähige, an Demenz erkrankte oder weitere kognitiv behinderte Menschen dürfte aber die Anforderung in Abs. 3 kaum einzuhalten sein. Deshalb ist für diese Fälle eine Präzisierung aufzunehmen.	[3] Die Auskunft muss für die betroffene Person verständlich sein, soweit dies im Rahmen des kognitiven Zustands möglich ist.
Art. 22	Die Frist von 30 Tagen ab Eingang des Begehrens um Dateneinsicht erscheint uns als vernünftig. Es stellt sich einzig die Frage, ob nicht die Gerichtsferien berücksichtigt werden sollten (namentlich die Sommermonate und Weihnachten, wegen vieler Absenzen).	-
Art. 23	Bei unverhältnismässig aufwändigen Auskunftserteilungen erscheint uns die auf CHF 300 angesetzte Obergrenze als viel zu tief. Wenn damit mehrere Arbeitstage an Aufwand anfallen, wäre nicht einmal ein Bruchteil der Kosten auf die Gesuchstellenden überwälzbar. Der Betrag sollte – auch gerade als Schutz vor querulatorischer Begehren – auf mindestens CHF 1'000 erhöht werden.	[1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. [2] Die Beteiligung beträgt maximal ~~300~~ 1'000 Franken.
Art. 25	Die Datenschutzgesetzgebung weist eine hohe Komplexität auf; deshalb sind ihre Anforderungen in der Praxis nicht immer einfach einzuhalten. Deswegen ist es sehr sinnvoll. Datenschutzberatende einzusetzen und die konkreten Modalitäten zu deren Einsatz im Sinne dieser Bestimmung festzulegen. Die Inhalte sind zu begrüssen, wie sie in dieser Bestimmung vorgeschlagen sind.	-
Art. 26 Bst. a + b	Die hier definierte und sehr sinnvolle Ausnahme einer Pflicht zur Führung eines Bearbeitungsverzeichnisses würde bei zahlreichen Betrieben nicht zur Anwendung kommen, weil: • in vielen Fällen die Betriebe besonders schützenswerte Personendaten in grossem Umfang bearbeiten; • aus einer Interpretation von Art. 20 Abs. 4, Art. 26 Abs. 3, Art. 31 Abs. 2 Bst. b nDSG hervorgeht, dass Art. 26 eVSDG auch Betriebe mit weniger als 250 Mitarbeitenden angewendet werden soll, wenn sie einem Konzern zugehören, der insgesamt mindestens 250 Mitarbeitende beschäftigt.	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:

	Um Rechtssicherheit zu gewährleisten und keinen unnötigen Aufwand für kleinere Betriebe (namentlich auch gerade im Gesundheitswesen) zu schaffen, ist eine Anpassung (messbare Präzisierungen) wichtig. Während wir die Unterstellung von Teilen der Konzerne nachvollziehen können, erscheint uns die «Bearbeitung von besonders schützenswerten Daten in grossem Umfang» als zu wenig präzise Konkretisierung. Wir beantragen deshalb eine Präzisierung, was unter «grossem Umfang» zu verstehen ist, nach unserer Ansicht wäre die Schwelle etwa bei 1'000 Datensätzen festzusetzen. Diesfalls erhält auch die Führung eines Verzeichnisses aber auf freiwilliger Basis mehr Gewicht, sie kann insbesondere bei regelmässiger Bearbeitung von Personendaten eine nützliche und einfache Tätigkeitsunterstützung darstellen: Dadurch können das Beibehalten eines Überblicks der Bearbeitungstätigkeiten und auch die Einhaltung anderer Verpflichtungen erleichtert werden.	a. Es werden umfangreich (mindestens 1000 Datensätze) besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.
Art. 45 Abs. 2	Die Zutrittsschwelle zum EDÖB ist niedrig zu halten, ganz besonders auch zur Überprüfung der Angemessenheit von Kodizes (Art. 59 Abs. 1 Bst. a nDSG) oder die Genehmigung von Standarddatenschutzklauseln (Art. 59 Abs. 1 Bst. b nDSG). Im Sinne einer rechtmässigen Umsetzung der komplexen neuen Datenschutzgesetzgebung sollte das Anrufen des EDÖB nicht durch das Erheben von Gebühren entgegengewirkt werden, ganz besonders für den Bereich der Gesundheitsbetriebe. Es gibt keinen nachvollziehbaren Grund, weshalb die Person, welche Dienstleistungen von ihm braucht, um sich datenschutzkonform zu verhalten, derart zur Kasse gebeten wird. Weder kann es sein, dass die Gebühren nach Zeitaufwand berechnet werden (die Privatperson hat keinen Ein-fluss auf die Effizienz der Leistungserbringung durch den EDÖB), noch sind die Stundensätze von CHF 150.00 bis 350.00 in irgendeiner Weise angemessen.	[2bis] Für Leistungserbringer nach Art. 35 Abs. 2 KVG wird auf die Erhebung von Kosten verzichtet. Alternativ: [2bis] Für Leistungserbringer nach Art. 35 Abs. 2 KVG gilt ein Stundenansatz von 50 bis 100 Franken.

Eidgenössisches Justiz-
und Polizeidepartement EJPD
3003 Bern

Per E-Mail an: Jonas.amstutz@bj.admin.ch

Bern, 14. Oktober 2021

Stellungnahme zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese hiermit gerne fristgerecht wahr.

asut, der Schweizerische Verband der Telekommunikation repräsentiert heute die Telekommunikationsbranche und sämtliche Wirtschaftszweige sind in ihm vertreten. Wir gestalten und prägen gemeinsam mit unseren Mitgliedern die digitale Transformation der Schweiz und setzen uns für optimale politische, rechtliche und wirtschaftliche Rahmenbedingungen für die digitale Wirtschaft ein. Die Telekombranche bearbeitet vorwiegend Daten und dabei teilweise auch sehr sensitive Daten. Es ist daher von grosser Relevanz für unsere Mitglieder, dass hier zeitnah Klarheit in Bezug auf das neue Datenschutzgesetz und der dazugehörigen Verordnung herrscht. Dies insbesondere auch mit Blick darauf, zu den Vorgaben der Europäischen Union Äquivalenz zu schaffen, was aus wirtschaftlicher und politischer Sicht nicht zu unterschätzen ist.

1 Grundsätzliche Bemerkungen

Wir möchten den Zeitplan der Umsetzung nicht gefährden, jedoch trotzdem auf bestehende Unstimmigkeiten im vorliegenden Entwurf der VDSG hinzuweisen. Auf eine völlige Neuausarbeitung des Entwurfes ist aus zeitlichen Gründen zu verzichten. Jedoch dürfen mit der Verordnung keine Vorgaben einfliessen, ohne dass eine gesetzliche Grundlage dafür vorhanden wäre. Die Verordnung ist darauf beschränkt, die gesetzlichen Vorgaben aus dem revDSG durch Detailvorschriften näher auszuführen und nicht neue gesetzliche Normen aufzunehmen. Insbesondere ist auf einen Swiss Finish und zusätzliche Restriktionen zu verzichten. Diese verbessern unseres Erachtens den Nutzen für die Konsumentinnen und Konsumenten nicht und verlangen der Wirtschaft einen unnötigen administrativen Mehraufwand ab. Aus Sicht der asut ist es zwingend, dass die Schweizer Datenschutzgesetzgebung von der EU als gleichwertig anerkannt wird, damit der grenzübergreifende Datenaustausch weiterhin effizient möglich bleibt.

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

@asut_ch

2 Spezifische Anpassungen oder Streichungen

2.1 Bestimmungen betreffend die Bundesorgane

Da sich im Entwurf diverse Vorgaben für die Bundesorgane analog denjenigen für Privatpersonen verändert haben oder sogar auf Private ausgeweitet wurden – was nicht einzusehen ist – sollen diese entsprechend angepasst oder falls notwendig gestrichen werden. asut unterstützt die Eingabe der Swico mit den Streichungs- und Anpassungsvorschläge vollumfänglich.

2.2 Bestimmungen betreffend die Privatpersonen

Mit Ausnahme der nachfolgend separat aufgeführten Artikel unterstützt asut die Eingabe der Swico.

Die Art. 17 (Überprüfung einer automatisierten Einzelentscheidung), Art. 18 (Form und Aufbewahrung der Datenschutz-Folgeabschätzung) und Art. 19 (Meldung von Verletzungen der Datensicherheit) möchten wir wie folgt kommentieren:

Art. 17: ist ersatzlos zu streichen
- Die Vorgaben im Zusammenhang mit automatisierten Einzelentscheidungen sind in Art. 21 revDSG bereits ausreichend und in Sinne einer risikobasierten Wertung definiert. Damit wird dem einzelnen Verantwortlichen auch bewusst ein angemessener Spielraum für die Umsetzung gewährt. Weitere Vorgaben, wie sie dem Entwurf entnommen werden können, stützen sich nicht auf eine gesetzliche Grundlage, weshalb sie zu streichen sind.
- Des Weiteren ist der Nebensatz «so darf sie deswegen nicht benachteiligt werden» unklar und erfüllt damit die Konkretisierung des Gesetzesartikels als zentrale Aufgabe der Verordnung nicht ansatzweise.

Art. 18: ist anzupassen
- Die Form der Datenschutz-Folgeabschätzung nur in schriftlicher Form zu verlangen, ist einerseits unklar, aber entspricht auch nicht mehr der heutigen Vorgehensweise in einer digitalisierten Welt.
- Die Aufbewahrungspflicht von zwei Jahren ist unseres Erachtens eine zu scharfe, aber auch unpräzise Definition. Es sollte hier dem Verantwortlichen überlassen werden, die Dauer der Aufbewahrungsfrist für den Einzelfall angemessen lang selber zu definieren, und zwar unter Berücksichtigung der entsprechenden Beweisrisikopflicht.

Formulierungsvorschlag:
Der Verantwortliche muss die Datenschutz-Folgeabschätzung in einer nachweisbaren Form für einen entsprechend angemessenen Zeitraum festhalten.

Art. 19: ist anzupassen, Absatz 5 ganz zu streichen
- Lit. e und f ist unseres Erachtens unklar formuliert, denn es sind gemäss Art. 24 Abs. 1 revDSG dem EDÖB Verletzungen zu melden, welche «voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt». Dies muss auch entsprechend in der Formulierung klar wiedererkennbar sein.
- Absatz 3 ist dahingehend einzuschränken, so dass es mit den Vorgaben von Art. 24 Abs. 4 revDSG übereinstimmt. Die Verordnung kann hier nicht weitergehen, als das Gesetz es verlangt.

Formulierungsvorschlag:
Lit. e: die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht;
Lit. f: welche allfälligen Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder das Risiko zu mildern;
Absatz 3: Sofern der Verantwortliche verpflichtet ist, die betroffenen Personen zu informieren, so teilt er ihnen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 mit.
Absatz 5: ersatzlos streichen

Wir danken ihnen bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Peter Grütter
Präsident

auto schweiz suisse

MENSCHEN · MÄRKTE · MOBILITÄT

Elektronische Einreichung:
fanny.matthey@bj.admin.ch

Bern, 6. Oktober 2021 / FL / bna

Revision der Datenschutzverordnung
Stellungnahme von auto-schweiz, Vereinigung Schweizer Automobil-Importeure

Sehr geehrte Frau Matthey
Sehr geehrte Frau Nüesch
Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, zu dem im Titel genannten Thema wie folgt Stellung nehmen zu dürfen. Unsere Stellungnahme entspricht inhaltlich derjenigen des Auto Gewerbe Verband Schweiz AGVS.

Am 25. September 2020 hat das Parlament – nach langen Debatten – die Totalrevision des Schweizer Datenschutzgesetzes (revDSG) verabschiedet. Dieses ist international abgestimmt, um dem EU-Standard (DSGVO) Rechnung zu tragen, und enthält daher im Wesentlichen keine Swiss Finishes. Damit schafft das Gesetz Rechtssicherheit für Schweizer Unternehmen, welche sich (auch) an die Bestimmungen der DSGVO halten müssen. **Der Entwurf der Verordnung zum Datenschutzgesetz (E-VDSG) gefährdet die gewonnene Rechtssicherheit durch zahlreiche Regelungen, welche weit über diejenigen der DSGVO hinausgehen. Zudem wurden Punkte in die E-VDSG aufgenommen, welche während der Debatten aus dem Gesetzesentwurf entfernt wurden.**

Wir bitten Sie, den Entwurf dahingehend zu überarbeiten, dass sämtliche Swiss Finishes und Widersprüche zum revDSG beseitigt werden. Die Verordnung hat sich auf Konkretisierungen des Gesetzes zu beschränken und darf insbesondere nicht Regelungen aufstellen, welche bewusst nicht in das Gesetz aufgenommen wurden (z.B. Art. 16 E-VDSG). Unsere nachfolgenden Forderungen und Formulierungsvorschläge in Bezug auf einzelne Artikel des Entwurfs sollen Ihnen bei der Überarbeitung dienen. Alle aufgeführten Punkte sind aus unserer Sicht grundsätzlich zwingend zu berücksichtigen (Prio 1: dunkelorange, Prio 2: hellorange, Prio 3: weiss).

Bei allfälligen Rückfragen stehen wir Ihnen gerne zur Verfügung

Freundliche Grüsse

François Launaz
Präsident

Andreas Burgener
Direktor

auto-schweiz
Vereinigung Schweizer Automobil-Importeure

Wölflistrasse 5 · CH-3006 Bern
T +41 (0) 31 306 65 65

www.auto.swiss
info@auto.swiss

Artikel	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag
Generell	Entgegen ihrer Natur als reine ***Ausführungs***verordnung zum Datenschutzgesetz enthält die E-VDSG Regelungen, welche über eine blosse Konkretisierung des revDSG hinausgehen.	Die VDSG hat ausschliesslich die Konkretisierung des revDSG zum Zweck (vgl. Erläuterungen, S. 9). Sie darf darüber hinaus keine zusätzlichen eigenen Regelungen vorsehen. Dies führte zu einer eigentlichen Parallelgesetzgebung.	Konsequente Streichung aller mit dem E-VDSG eingeführten **Swiss Finishs** (vgl. nachfolgend). Ergänzung der Titel in der Verordnung mit einer Verweisung auf die entsprechende gesetzliche Grundlage. Z.B.: „Art. 1 Grundsätze (Art. 8 Abs. 3 DSG)“
	Die zusätzlich aufgestellten Regelungen entbehren nicht nur einer Rechtsgrundlage im Gesetz, wo der Gesetzgeber teilweise bewusst anders entschieden hat, sondern gehen auch über das Niveau der DSGVO hinaus. Diese **Swiss Finishs** stehen aber im Widerspruch zur expliziten Zielsetzung des Gesetzgebers und auch des BJ, wonach Kompatibilität mit der DSGVO geschafft werden sollte (Erläuterungen, S. 10).	Wie das BJ in den Erläuterungen (S. 10) selbst ausführt, soll durch Kompatibilität mit der DSGVO Rechtssicherheit für Unternehmen geschaffen werden, welche sich an die DSGVO halten. Das gelingt freilich nicht, wenn die VDSG gegenüber dem revDSG (neue) **Swiss Finishs** einführt. Im Gegenteil, damit sind Doppelspurigkeiten und Widersprüche vorprogrammiert.	
1	Berücksichtigung des Implementierungsaufwands statt der -kosten als Kriterium aufnehmen.	Die Erläuterungen zur Berücksichtigung der Implementierungskosten als Kriterium bei der Beurteilung der Angemessenheit sind u.E. unpräzise (vgl. Erläuterungen, S. 16). Entgegen diesen Ausführungen sind die Implementierungskosten gemäss E-VDSG 1 I b bei der Beurteilung der Frage, ob eine Massnahme angemessen ist, zu berücksichtigen, und nicht erst, wenn es darum geht, sich für eine von mehreren angemessenen Massnahmen zu entscheiden. Zudem ist nicht allein auf die Implementierungs*kosten*, sondern generell auf den Implementierungs*aufwand* abzustellen. Das sollte in der Verordnung entsprechend präzisiert werden.	1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a.–c. […]; d. Implementierungs~~kosten~~*aufwand*. ~~2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.~~ **Eventualiter:** 1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a.–c. […]; d. Implementierungs~~kosten~~*aufwand*.
	Streichung der Pflicht zur Überprüfung in angemessenen Abständen.	Die Pflicht zur Überprüfung in angemessenen Abständen nach VDSG 1 II hat keine Grundlage im revDSG.	

	Eventualiter: Pflicht zur Überprüfung der Massnahmen in angemessener *Weise*	**Eventualiter:** Wenn, dann sind die Massnahmen infolge risikobasierten Ansatzes nicht in angemessenen *Abständen*, sondern vielmehr in angemessener *Weise* zu überprüfen. Denn die Frage, ob eine Kontrolle nötig ist, hängt insbesondere davon ab, ob sich die Risiken geändert haben. Zeitliche Aspekte sind irrelevant.	2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen~~r~~ ~~Abständen~~ *Weise* zu überprüfen.
3	Die Protokollierungspflicht nach VDSG 3 ist zu streichen. **Eventualiter:** Einschränkung auf Fälle, wo ohne Protokollierung nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden (vgl. auch geltender Art. 10 Abs. 1 VDSG).	Die Protokollierungspflicht nach VDSG 3 hat keine Grundlage im revDSG und widerspricht dem risikobasierten Ansatz. Auch „hohen" Risiken ist mit den im Einzelfall *adäquaten Massnahmen* zu begegnen. Die DSGVO sieht keine Protokollierungspflicht vor. Es handelt sich daher um einen **Swiss Finish**. Auf einer Dokumentationspflicht, wie sie im VE-DSG vorgesehen war, wurde aufgrund der Eingaben in der Vernehmlassung verzichtet bzw. sie wurde durch die Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen ersetzt. Diese geht weiter als die bisherige Pflicht zur Anmeldung der Datensammlung beim EDÖB. Es müssen neu alle Bearbeitungen in einem Verzeichnis aufgeführt sein. Es nicht erforderlich, an der Protokollierungspflicht festzuhalten. Die Einführung der Protokollierungspflicht als Teil der Datensicherheit hätte stossende Auswirkungen: Falls trotz gegebenen Voraussetzungen keine DSFA durchgeführt wird, so hat dies gemäss revDSG *keine* Sanktion zur Folge.	**Streichung von VDSG 3**, zumindest für den Privatbereich. **Eventualiter:** 1 Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht *und kann sonst nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden,* protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. 2 […] 3 […] 4 […]

		Wird hingegen eine DSFA durchgeführt, aber in der Folge gegen die allfällige Protokollierungspflicht (als Teil der Datensicherheit) verstossen, so ist das sanktionsbedroht. Der Verantwortliche hat die vorgängig Stellungnahme des EDÖB einzuholen, wenn sich aus der DSFA ergibt, dass eine geplante Bearbeitung trotz Massnahmen ein hohes zur Folge hat. Der EDÖB kann dem Verantwortlichen bei etwaigen Einwänden (angemessene) ebenfalls Massnahmen vorschlagen.	
4	Die Pflicht zur Erstellung eines Reglements nach VDSG 4 ist zu streichen. **Eventualiter:** Falls an dieser Regelung festgehalten werden sollte, müsste zumindest präzisiert werden, dass die Angaben gemäss Abs. 2 einzig in Bezug auf Bearbeitungen gemacht werden müssen, welche unter Art. 1 Abs. 1 lit. a und/oder b fallen.	Die Pflicht zur Erstellung eines Reglements nach VDSG 4 I hat keine Grundlage im revDSG und widerspricht dem risikobasierten Ansatz. Auch „hohen" Risiken ist mit den im Einzelfall *adäquaten* Massnahmen zu begegnen. Die DSGVO sieht keine Pflicht zur Erstellung eines Reglements vor. Es handelt sich daher um einen **Swiss Finish**. Auf einer Dokumentationspflicht, wie sie im VE-DSG vorgesehen war, wurde aufgrund der Eingaben in der Vernehmlassung verzichtet bzw. sie wurde durch die Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen ersetzt. Diese geht weiter als die bisherige Pflicht zur Anmeldung der Datensammlung beim EDÖB. Es müssen neu alle Bearbeitungen in einem Verzeichnis aufgeführt sein. Es nicht erforderlich, an der praxisfernen Pflicht zur Erstellung eines Reglements festzuhalten.	**Streichung von VDSG 4**, zumindest für den Privatbereich.
6	Unklar, was die Ausführungen auf S. 24 der Erläuterungen zu den Anforderungen an den Inhalt des ADV gemäss Art. 22 Abs. 3 DSGVO bezwecken, zumal diese in Art. 6 E-VDSG nicht vorgesehen sind.	Diese Ausführungen suggerieren, dass der ADV gemäss VDSG 6 den inhaltlichen Anforderungen der DSGVO genügen müsse. Hierfür findet sich indes keine gesetzliche Grundlage. Auch die E-VDSG enthält keine inhaltlichen Vorgaben.	Klarstellung im Erläuterungsbericht, dass die VDSG – anders als die DSGVO – keinen Mindestinhalt an den ADV vorschreibt.

	Streichung der Pflicht zur Sicherstellung einer vertrags- oder gesetzesgemässen Bearbeitung.	„Sicherstellung“ der vertrags- und gesetzesgemässen Bearbeitung ist nicht möglich. Analog DSGVO 28 I kann der Verantwortliche nur, aber immerhin verpflichtet werden, nur Auftragsbearbeiter zu beauftragten, welche durch angemessene Massnahmen die Bearbeitung im Einklang mit den Anforderungen des revDSG und den Schutz der Rechte der Betroffenen gewährleisten.	1 Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. ~~Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.~~ *Er arbeitet nur mit Auftragsbearbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen so durchgeführt werden, dass die Bearbeitung im Einklang mit den Anforderungen der Schweizer Datenschutzgesetzgebung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.* 2 ~~Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.~~ 3 Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich *oder in einer anderen Form, die den Nachweis durch Text ermöglicht,* genehmigt hat.
	Streichung von Abs. 2, weil der Auslandtransfer separat geregelt ist.	Abs. 2: Auslandtransfers sind separat geregelt (E-VDSG 8), weshalb für diese Regelung keine Notwendigkeit besteht. Sollte an dieser Regelung festgehalten werden, so wäre im letzten Satz zu präzisieren, dass „andernfalls ein geeigneter Datenschutz gemäss Art. 16 Abs. 2 revDSG zu gewährleisten ist.“	
	Präzisierung des Begriffs „schriftlich“, der auch „in Text nachweisbare Formen“ umfasst.	Abs. 3: „Schriftlich“ dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	

10	Der Empfänger kann nicht verpflichtet werden, „die schweizerischen Datenschutzvorschriften“ einzuhalten. Das ist im Erläuterungsbericht klarzustellen.	Im Erläuterungsbericht (S. 28) ist festgehalten, dass der Empfänger verpflichtet werden müsse, „die schweizerischen Datenschutzvorschriften“ einzuhalten. Das ist unzutreffend; er muss die Standardklauseln einhalten, nicht jedoch Schweizer Datenschutzrecht. So verlangt auch E-VDSG 6 II, dass der Auftragsbearbeiter „gleichwertige“ Bestimmungen einhalten muss.	Klarstellung im Erläuterungsbericht, dass der Empfänger nicht verpflichtet werden muss, „die schweizerischen Datenschutzvorschriften“ einzuhalten.
	Ersatz des Begriffs „Sicherstellung“ durch „darauf hinwirken“.	Der Exporteur kann nicht „sicherstellen“, dass der Empfänger die Standarddatenschutzklauseln beachtet; er kann nur, aber immerhin darauf hinwirken.	1 Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um ~~sicherzustellen~~ *darauf hinzuwirken*, dass die Empfängerin oder der Empfänger diese beachtet. *Die Angemessenheit der Massnahmen richtet sich nach den Umständen im konkreten Fall und dem Stand der Technik.* 2 […]
	Präzisierung, dass sich die Angemessenheit der geforderten Massnahmen nach den Umständen im konkreten Einzelfall richte und die Anforderungen insb. dann höher seien, wenn es sich um besonders schützenswerte Personendaten handle.	Dies ist in den Erläuterungen (S. 28) unter Hinweis auf das BJ entsprechend festgehalten und sollte zur Klarstellung auch in die Verordnung einfliessen. Der risikobasierte Ansatz bei der Beurteilung von Datentransfers in Länder ohne angemessenen Datenschutz auf Grundlage der SCC ist zu bejahen. Allerdings ist dieser Ansatz mit Blick auf die Praxishinweise der EU-Behörden keinesfalls selbstverständlich. Entsprechend bedarf es einer Klarstellung in der Verordnung zur Schaffung von Rechtssicherheit.	
NEU	Präzisierung des räumlichen Anwendungsbereichs des revDSG (Auswirkungsprinzip, Art. 3 I):	Gemäss revDSG 3 I gilt das Gesetz für Sachverhalte, die sich in der Schweiz auswirken auch wenn sie im Ausland veranlasst werden. Weder das Gesetz noch die Verordnung halten fest, ob an die Auswirkungen weitere Anforderungen zu stellen sind. Eine solche qualifizierte Auswirkung (Spürbarkeit) ist erforderlich, um Übertreibungen bei der extraterritorialen Anwendung des Schweizer Datenschutzrechts vorzubeugen. Hierzu ist eine Regelung analog zum Marktortprinzip gemäss DSGVO aufzunehmen.	*Folgende Sachverhalte, die im Ausland veranlasst werden, wirken sich in der Schweiz aus:* *a. das Angebot von Waren oder Dienstleistungen gegenüber betroffenen Personen in der Schweiz;* b. *die Beobachtung des Verhaltens von betroffenen Personen, soweit ihr Verhalten in der Schweiz erfolgt.*
13	Richtigstellung, dass keine „Basisinformationen“ auf der ersten Kommunikationsstufe mitgeteilt werden müssen.	Das revDSG sieht nicht vor, dass die Betroffenen die „wichtigsten Informationen“ auf der „ersten Kommunikationsstufe“ erhalten müssen (vgl. aber Erläuterungen,	Richtigstellung im Erläuterungsbericht, dass den Betroffenen keine „Basisinformationen“ auf der ersten Kommunikationsstufe mitgeteilt werden müssen und

		S. 30). Vielmehr hält revDSG 19 I fest, die Information müsse „angemessen" erfolgen. Daraus folgt, dass das die Mitteilung von den jeweiligen Umständen abhängig ist. Dabei sind auch Informationsinteresse und die Erwartungen des Betroffenen zu berücksichtigen: Während er damit rechnen mag, dass sich in einem Vertrag ein Hinweis auf den die Datenschutzerklärung findet, ist ein solcher auf Visitenkarten, E-Mails oder Briefpapier nicht üblich. Sollte sich eine Person dafür interessieren, kann ihr zugemutet werden, die Webseite des betreffenden Unternehmens zu konsultieren. Darum darf es nicht erforderlich sein, in Alltagssituationen – wie bei einer Terminvereinbarung, am Schalter – explizit auf die Datenschutzerklärung hinweisen zu müssen (s. Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 99). Zudem wäre ohnehin unklar, welches die „wichtigsten Informationen" sind.	dass auch das Informationsinteresse der Betroffenen im Einzelfall zu berücksichtigen ist.
	Streichung der gesetzlich nicht vorgesehenen Informationspflicht des Auftragsbearbeiters.	Der Auftragsbearbeiter hat gemäss revDSG keine Informationspflicht (vgl. revDSG 19). Eine solche kann nicht in der VDSG eingeführt werden.	**Streichung von Art. 13 VDSG** **Eventualiter:** ~~1~~ Der Verantwortliche ~~*und der Auftragsbearbeiter teilen*~~ *teilt* die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit. *Als leicht zugänglich gilt insbesondere die Information, welche auf der Webseite des Verantwortlichen abrufbar ist.* ~~2 Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~
	Streichung der unpräzisen Vorgaben für eine angemessene Information. Streichung der unklaren Anforderungen an Piktogramme.	Weil Piktogramme ohnehin nur ergänzend verwendet werden dürfen, sind daran keine zusätzlichen Anforderungen zu stellen. Zumal aufgrund der Erläuterungen nicht klar ist, was mit „maschinenlesbar" gemeint ist.	
15	Die Informationspflicht bei der Bekanntgabe von Personendaten ist zu streichen.	Diese Informationspflicht entbehrt einer Grundlage im revDSG. Auf die Richtlinie (EU) 2016/680 (Schengen-RL) ist für den Privatbereich nicht abzustellen. Die DSGVO sieht	**Streichung von Art. 15.**

		keine entsprechend Pflicht vor. Eine Umsetzung ist nicht erforderlich und schafft einen **Swiss Finish**. Der Auftragsbearbeiter ist gemäss revDSG wie bereits erwähnt nicht Adressat der Informationspflicht. Keine Notwendigkeit: Der Verantwortliche hat bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten.	
16	Die Informationspflicht über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten ist zu streichen.	Diese Informationspflicht entbehrt einer Grundlage im revDSG. Diese Pflicht wurde im Vorentwurf des DSG vorgeschlagen, im Rahmen der Vernehmlassung jedoch wieder gestrichen. Sie darf entsprechend nicht über die VDSG wieder eingeführt werden. Keine Notwendigkeit: Der Verantwortliche hat bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten.	**Streichung von Art. 16.**

18	Analog DSGVO 35 IV soll der EDÖB eine Liste erstellen und publizieren, welche Bearbeitungen enthält, für die eine bzw. keine DSFA zu erfolgen hat. Alternativ oder kumulativ sind Kriterien zu nennen, wonach ermittelt werden kann, ob eine DSFA durchzuführen ist oder nicht. „Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	Ohne Kriterien und/oder Liste mit Beispielen von Bearbeitungen, die eine DSFA erfordern bzw. nicht erfordern, besteht eine grosse Rechtsunsicherheit.	*1 Der Beauftragte erstellt eine Liste mit Bearbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Er kann zusätzlich eine Liste mit Bearbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.* *2* Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich *oder in einer anderen Form, die den Nachweis durch Text ermöglicht,* festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~
	Die Aufbewahrungsfrist ist zu streichen.	Die Dokumentationspflicht gemäss VDSG 18 entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Zudem besteht der Anreiz, der Dokumentationspflicht nicht nachzukommen, da diese – im Gegensatz zu einer Verletzung der Datensicherheit – nicht strafbar ist. Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelungen einen **Swiss Finish** darstellen.	
	Der Begriff der Schriftlichkeit ist zu präzisieren.	„Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	

19	Die Auslegung des Begriffs „voraussichtlich“ ist falsch und zu korrigieren.	„Voraussichtlich“ heisst nicht, dass „in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen kann, eine Meldung erfolgen muss“ (so die Erläuterungen, S. 32). Der Begriff „voraussichtlich“ setzt vielmehr voraus, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko führt.	Richtigstellung im Erläuterungsbericht, dass in Fällen, wo das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, nicht gemeldet werden muss, sondern nur dann, wenn die Verletzung der Datensicherheit **höchstwahrscheinlich** zu einem hohen Risiko führt.
	Streichung der in der Verordnung gegenüber dem Gesetz zusätzlich eingeführten Mindestangaben bei einer Meldung einer Verletzung der Datensicherheit.	Gemäss revDSG 24 II hat der Verantwortliche in der Meldung einer Verletzung der Datensicherheit „mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen zu [nennen]“. Die E-VDSG sieht weitere Mindestangaben vor. Die DSGVO sieht keine Angabe von Zeitpunkt und Daher der Verletzung vor. Es handelt sich daher um einen **Swiss Finish**.	1 Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit: a. die Art der Verletzung; ~~b. soweit möglich den Zeitpunkt und die Dauer;~~ ~~c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;~~ ~~d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;~~ e.-g. […] 2 […] *3* ~~Der~~ *Falls der* Verantwortliche *verpflichtet ist, die* ~~teilt den~~ betroffenen Personen *zu informieren, so teilt er ihnen* in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit. 4 […] ~~5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.~~
	Streichung der über das Gesetz hinausgehenden generellen Pflicht, die betroffene Person zu informieren.	E-VDSG 19 II geht über revDSG 20 IV hinaus. Während das Gesetz eine Information der betroffenen Person nur vorschreibt, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt, sieht die Verordnung vor, dass der Verantwortliche den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mitteilt.	
	Streichung der gesetzlich nicht vorgesehenen Dokumentationspflicht nach VDSG 19 V.	Dokumentationspflicht nach VDSG 19 V entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie nach der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor. Es handelt sich daher um einen **Swiss Finish**. Falls an der Dokumentationspflicht festgehalten werden sollte, ist zu präzisieren, dass nur meldepflichtige Verletzungen aufzubewahren sind.	

20	Die Auskunftserteilung sollte nicht nur schriftlich, sondern auch in einer anderen durch Text nachweisbaren Form möglich sein.	In den Erläuterungen (S. 34) wird festgehalten: „Es kann hier ferner präzisiert werden, dass zur schriftlichen Form auch die elektronische Form gehört." Diese Präzisierung ist in die Verordnung aufzunehmen.	1 […] 2 Die Auskunft wird in der Regel schriftlich *oder in einer Form, die den Nachweis durch Text ermöglicht,* erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat. 3-4 […] *5 Die betroffene Person hat keinen Anspruch auf Herausgabe von Dokumenten, selbst wenn diese Personendaten enthalten sollten.* ~~5 Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.~~
	Aufnahme der Präzisierung, dass der Begriff „Daten als solche" insbesondere auch eine Auskunft in aggregierter Form zulässt.	In den Erläuterungen (S. 35) wird ausgeführt: „Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Die mündliche Mitteilung von Informationen, zum Beispiel am Telefon, ist ebenfalls möglich, sofern die betroffene Person eingewilligt hat." Es besteht im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten bzw. Unterlagen. Vielmehr ist die Mitteilung nach entsprechender Debatte vom Gesetzgeber bewusst beschränkt worden auf die bearbeiteten Personendaten „als solche" (revDSG 25 II b). Damit soll namentlich auch die Auskunft in aggregierter Form ermöglicht werden. Dies sollte zwecks Präzisierung in der Verordnung verankert werden.	
	Dokumentationspflicht nach VDSG 20 V ist zu streichen.	Dokumentationspflicht nach VDSG 20 V entbehrt einer gesetzlichen Grundlage(vielmehr wurde sie im Rahmen	

		der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen **Swiss Finish** darstellen. Die Regelung ist ferner unnötig, da aufgrund der Beweislast ohnehin im Interesse des Verantwortlichen mit Dokumentation den Nachweis erbringen zu können.	
22	Der Fristenbeginn ist zu präzisieren.	Präzisierung erforderlich: Wenn aus dem Auskunftsbegehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.	1 Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen. *Wenn aus dem Begehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.* 2 […]
23	Erhöhung der Beteiligung an den Kosten für eine Auskunftserteilung.	Eine wesentliche Erhöhung der Beteiligung des Betroffenen ist angezeigt, weil der geltende Betrag von CHF 300.00 regelmässig in keinem Verhältnis zum Aufwand steht.	1 […] 2 Die Beteiligung beträgt maximal *5'000.00* Franken. 3 […]
24	Klarstellung, dass „Datenportabilität" kein Zwang zu standardisierten Datenbearbeitungssystemen beinhaltet.	Die „Datenportabilität" wurde erst im Rahmen der parlamentarischen Debatte eingeführt. Entsprechend enthält die Botschaft keine Ausführungen dazu. Die Verordnung muss hier Konkretisierungsarbeit leisten.	*1 Das Recht der betroffenen Person, sie betreffende Personendaten vom Verantwortlichen heraus zu verlangen oder durch diesen an einen anderen Verantwortlichen übertragen zu lassen, begründet für den Verantwortlichen nicht die Pflicht, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten.* *2* […]
26	Es ist zu präzisieren, dass sich die allfällige Pflicht eines KMU zur Führung eines Verzeichnisses nicht auf sämtliche Bearbeitungen erstreckt, sondern auf diejenigen Bearbeitungen beschränkt ist, welche die Voraussetzung(en) triggern.	Der Bundesrat hat gemäss revDSG 12 V Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses vorzusehen für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und deren Datenbearbeitung ein „geringes Risiko" mit sich bringt. Gemäss E-VDSG 26	*1* Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürli-

		bedeutet ein geringes Risiko, dass weder „umfangreich besonders schützenswerte Personendaten bearbeitet“ werden noch „ein Profiling mit hohem Risiko durchgeführt“ wird. Alle anderen Bearbeitungen bringen im Umkehrschluss ein geringes Risiko mit sich. Durch Präzisierung, dass sich die Pflicht zur Führung eines Verzeichnisses ausschliesslich auf diejenigen Bearbeitungen erstreckt, welche die Voraussetzung triggern, kann sowohl dem Schutz der betroffenen Personen als auch den Bedürfnissen der KMU angemessen Rechnung getragen werden (vgl. auch das Positionspapier des EDSA zu Art. 30 Abs. 5 DSGVO).	che Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. […] b. […] *2 Ist eine Voraussetzung nach Abs. 1 Bst. a und/oder b erfüllt, so ist die Verzeichnispflicht auf diejenige bzw. diejenigen Bearbeitungen beschränkt, welche dieser bzw. diesen Voraussetzung bzw. Voraussetzungen zugrunde liegen.* *3 Das Bearbeitungsverzeichnis ist schriftlich, oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu führen.*
	Es ist ferner zu präzisieren, dass das Verzeichnis nicht schriftlich, sondern auch in anderer Form, die den Nachweis durch Text ermöglicht, z.B. elektronisch, geführt werden kann.	Damit ist klargestellt, dass das Verzeichnis auch elektronisch geführt werden kann.	

Dr. Rehana Chandrika Harasgama
Rechtsanwältin
+41 58 261 50 00
rehana.harasgama@baerkarrer.ch

BÄR & KARRER

Postfach 1548 | CH-8002 Zürich

Per email (daniela.nueesch@bj.admin.ch; fanny.matthey@bj.admin.ch)

Bundesamt für Justiz
z.Hd. Frau Danielle Schneider und Frau
Fanny Matthey
Bundesrain 20
CH-3003 Bern

Zürich, 14. Oktober 2021
[ProjectNo]/2131_Telephone]/bk/

Vernehmlassung zur Revision der Verordnung zum totalrevidierten Bundesgesetz über den Datenschutz

Sehr geehrte Damen und Herren

Wir beziehen uns auf Ihre Medienmitteilung vom 23. Juni 2021 und danken Ihnen für die Gelegenheit, zur Revision der Verordnung zum Bundesgesetz über Datenschutz ("**rVDSG**") im Rahmen der Totalrevision des Datenschutzgesetzes ("**rDSG**") Stellung nehmen zu dürfen.

Gerne lassen wir Ihnen unsere Stellungnahme per E-Mail als pdf und word zukommen.

A Zusammenfassung

1 Am 25. September 2020 hat das Parlament das rDSG verabschiedet. Gemäss Medienmitteilung vom 23. Juni 2021 müssen zahlreiche Bestimmungen des rDSG in einer Verordnung konkretisiert werden, weshalb der Bundesrat am 23. Juni 2021 den Vorentwurf zur rVDSG in Vernehmlassung geschickt hat.

2 Wir gehen mit dem Bundesrat einig, dass gewisse Bestimmungen des rDSG in der rVDSG präzisiert werden müssen und zwar vor allem dort, wo das rDSG Ausführungsbestimmungen vorbehält oder wo Datenbearbeiter zusätzliche Informationen

und Konkretisierungen benötigen, um ihren Rechten und Pflichten gemäss rDSG nachkommen zu können.

3 Während wir den Vorschlag des Bundesrates insbesondere in Bezug auf die Bestimmungen zu Auslanddatentransfers, zum Datenschutzberater und zum Auskunftsrecht grundsätzlich begrüssen, sehen wir auch für einige Bestimmungen Verbesserungspotenzial; sei dies, weil unserer Ansicht nach eine gesetzliche Grundlage für die im Vorentwurf der rVDSG enthaltenen Bestimmungen fehlt, diese Bestimmungen über blosse Detailvorschriften zum Gesetz hinausgehen (BGE 141 II 169) oder weil gewisse Ausführungsbestimmungen in der Praxis zu grossen Umsetzungsschwierigkeiten führen würden.

4 Insbesondere die Bestimmungen zur Datensicherheit und zu den Dokumentations- und Informationspflichten sollten nach der Vernehmlassung genau geprüft und entweder – wie unten vorgeschlagen – ersatzlos gestrichen, präzisiert oder es sollten praktikablere Lösungen implementiert werden. Auch in Bezug auf die Auftragsdatenbearbeitung sowie das Recht auf Datenherausgabe oder -übertragung müssen unserer Ansicht nach gewisse Details angepasst oder präzisiert werden. Schliesslich sind wir der Ansicht, dass die rVDSG nicht unreflektiert Pflichten der aktuellen VDSG oder EU Datenschutzgrundverordnung ("**EU DSGVO**") übernehmen sollte, zumal das rDSG viele Änderungen enthält, welche die Übernahme solcher Pflichten nicht länger notwendig machen, wie z.B. die Pflicht zur Erstellung eines Bearbeitungsreglements.

B Allgemeine Bemerkungen

5 Im Rahmen unserer Stellungnahme befassen wir uns ausschliesslich mit den Artikeln in der rVDSG, welche private Datenbearbeiter betreffen. Unsere Aussagen beziehen sich entsprechend nicht auf die Bestimmungen für Bundesorgane, ausser es handelt sich um eine Bestimmung, die sowohl Private als auch Bundesorgane betrifft.

6 Nachfolgend fassen wir unsere allgemeinen Bemerkungen zu den vier von uns identifizierten Kernpunkten des Vorentwurfs zusammen. Danach haben wir in einer Tabelle zusätzliche Anpassungsvorschläge für bestimmte Artikel der rVDSG aufgelistet, auf welche wir jedoch nicht detailliert eingehen.

I Datensicherheit

7 Grundsätzlich begrüssen wir, dass im revidierten Datenschutzgesetz und demnach auch in der rVDSG die Datensicherheit gestärkt werden soll. Entsprechend ist es auch begrüssenswert, dass der Bundesrat in der rVDSG seiner Pflicht nach Art. 8 Abs. 3 rDSG im Rahmen der **Art. 1-5 rVDSG** nachkommen möchte. Zudem sind wir mit der Einschätzung des Bundesrates einverstanden, dass die Datensicherheit

je nach Unternehmen unterschiedlich ausgestaltet werden muss, um den mit der entsprechenden Unternehmenstätigkeit zusammenhängenden Risiken genügend Rechnung zu tragen (Erläuternder Bericht, S. 24). So steht im Erläuternden Bericht denn auch, dass die Verordnung keine "*starren Mindestanforderungen*" vorgibt, sondern einen risikobasierten Ansatz verfolgt, da es nicht möglich sei, allgemeingültige Mindestanforderungen für jegliche Branche festzulegen (Erläuternder Bericht, S. 10 und 14). Vor diesem Hintergrund verstehen wir auch, dass der Bundesrat mit der Bestimmung von Mindestanforderungen in der rVDSG für die Datensicherheit grundsätzlich zurückhaltend war.

8 Da jedoch gemäss Art. 61 lit. c rDSG bei Nichterfüllung der gemäss Art. 8 Abs. 3 rDSG definierten Mindestanforderungen eine Busse bis CHF 250'000.- drohen kann, scheinen uns die vorgeschlagenen Bestimmungen insbesondere in **Art. 1 und 2 rVDSG** nicht vollständig ausreichend, da nur allgemeine Schutzziele beschrieben werden, die gemäss Wortlaut zu erreichen sind. Gerade strafbewehrte Vorschriften müssen das inkriminierte Verhalten aber als Ausfluss des Legalitätsprinzips klar umschreiben.

9 So stellt sich einerseits die Frage, wie ein Unternehmen demonstrieren kann, dass es die definierten Schutzziele erreicht hat und somit seine Pflicht, die vom Bundesrat erlassenen Mindeststandards einzuhalten, erfüllt hat. Im Erläuterndem Bericht steht, dass Unternehmen in der Lage sein müssen, zu begründen, weshalb ein Schutzziel in einem Fall nicht von Relevanz ist (Erläuternder Bericht, S. 17). Ob diese Pflicht auch als Mindeststandard zu qualifizieren ist und somit ebenfalls strafbewehrt wäre, ist ebenfalls unklar.

10 Schliesslich ist auch unklar, ob die ausgebaute Protokollierungspflicht sowie die Pflicht zur Erstellung eines Bearbeitungsreglements gemäss **Art. 3 und 4 rVDSG** auch als Mindeststandard gelten und somit bei Nichterfüllung auch strafbewehrt wären. Beide Pflichten fanden schon im aktuell gültigen DSG keine eigentliche Rechtsgrundlage, weshalb es nicht sinnvoll erscheint, diese so in der rVDSG zu übernehmen oder gar auszubauen (siehe detaillierte Ausführungen unten in Rz. 14 ff.).

11 Wir regen an, dass der Bundesrat die Bestimmungen zur Datensicherheit vor diesem Hintergrund nochmals detailliert prüft und **entweder (i) rudimentäre und allgemeine Mindeststandards nach dem Vorbild von Art. 32 Abs. 1 lit. a-d EU DSGVO, die für alle Branchen gleichermassen gelten sollen, in der rVDSG definiert, oder zumindest präzisiert, welche Massnahmen in Frage kommen, um die definierten Schutzziele zu erfüllen** (wie dies im Erläuternden Bericht (S. 18–19) auch beschrieben wird, aber nicht in die rVDSG Eingang gefunden hat) **oder aber (ii), wenn die als "Schutzziele" bezeichneten Massnahmen die tatsächlich zu erfüllenden "Mindestanforderungen" sind, den Titel von Art. 2 rVDSG entsprechend anpasst**.

II Dokumentations- und Informationspflichten

1 Dokumentationspflichten

12 Die rVDSG enthält zahlreiche Informations- und Dokumentationspflichten, welche nicht nur die Pflichten gemäss rDSG ausführen, sondern teilweise neue Pflichten begründen. Dies ist erstaunlich, zumal der Bundesrat sich entgegen Art. 5 EU DSGVO dazu entschieden hat, keine allgemeine Dokumentationspflicht im rDSG aufzunehmen, sondern primär die Pflicht zur Führung eines Datenverzeichnisses. Entsprechend scheinen die neuen Dokumentationspflichten, die in die rVDSG aufgenommen wurden, unseres Erachtens dem Willen des Gesetzgebers zuwiderzulaufen.

13 Wie oben bereits kurz beschrieben, haben sowohl die in der rVDSG festgelegte Protokollierungspflicht (Art. 3 rVDSG) sowie die Pflicht, ein Bearbeitungsreglement zu erstellen (Art. 4 rVDSG), grundsätzlich keine gesetzliche Grundlage.

14 **Zur Protokollierungspflicht**: Private Datenbearbeiter sollen eine Pflicht zur Protokollierung bestimmter Datenbearbeitungsvorgänge haben, wenn eine Datenschutz-Folgenabschätzung ("**DSFA**") ergibt, dass durch eine automatisierte Bearbeitung von Personendaten trotz vorgesehener Massnahmen ein hohes Risiko für die Persönlichkeit und Grundrechte der betroffenen Personen besteht (**Art. 3 Abs. 1 rVDSG**). Unserer Ansicht nach wird ein Verantwortlicher kaum je eine Datenbearbeitung vornehmen, die nach einer DSFA weiterhin ein hohes Risiko darstellt, und zwar nur schon aus dem Grund, dass dies wohl gerechtfertigt sein müsste, und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte in einem solchen Fall konsultiert werden müsste (Art. 23 rDSG). Vor diesem Hintergrund macht die Einführung einer Protokollierungspflicht unseres Erachtens wenig Sinn.

15 Eine ähnliche Pflicht gibt es ohnehin bereits in Art. 10 VDSG, und die Protokollierung von Bearbeitungsschritten ist in der Praxis weit verbreitet. Praxisfremd scheint hingegen, dass die Protokolle gemäss Art. 3 Abs. 3 rVDSG nun "*getrennt vom System, in welchem die Personendaten bearbeitet werden*", aufbewahrt werden müssen. Eine getrennte Aufbewahrung der Protokolle ist aufwändig und technisch nicht ohne Weiteres umsetzbar, denn Protokolle fallen normalerweise dort an, wo sie erstellt werden und nicht auf anderen Systemen. Um der Pflicht zur getrennten Aufbewahrung zu entsprechen, müssten die Protokolle also extrahiert und auf andere Systeme verschoben werden. Dies muss durch entsprechende automatisierte Prozesse sichergestellt werden. Unklar ist auch, was mit einem "*getrennten System*" gemeint ist. Müssen die Protokolle von einem auf ein anderes System verschoben werden, sind die Systeme notwendigerweise auf eine gewisse Weise verbunden. Die getrennte Aufbewahrung ist unserer Meinung nach gesamtheitlich betrachtet als zu wenig konkretisiert und unverhältnismässig einzustufen. **Wir regen an, dass dieser Teilsatz von Art. 3 Abs. 4 ersatzlos gestrichen wird**.

16 Zudem ist auch nicht ersichtlich, warum diese Protokolle nun neu zwei Jahre aufbewahrt werden müssen und nicht mehr ein Jahr. **Wir regen grundsätzlich an, die Aufbewahrungsfristen in der rVDSG zu streichen oder zu vereinheitlichen** (siehe nachfolgend Rz. 19 f.). Schliesslich sollen die Protokolle nur den Personen zugänglich sein dürfen, "*denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit obliegen*" und die Protokolle sollen nur zu diesem Zweck verwendet werden dürfen. Private Datenbearbeiter können aber unterschiedliche Interessen haben, um ein solches Protokoll zu führen, weshalb es teilweise auch anderen Personen zugänglich gemacht werden muss und auch anderen Zwecken dienen können muss, solange die Datenbearbeitungsgrundsätze nach Art. 6 rDSG eingehalten werden. **Wir regen an, den zweiten Satz von Art. 3 Abs. 4 rVDSG ersatzlos zu streichen.**

17 **Zum Bearbeitungsreglement**: Obwohl viele Unternehmen eine Art Richtlinie betreffend Umgang mit Personendaten im Unternehmen implementiert haben, ist es in der Praxis nicht sehr weit verbreitet, ein derart detailliertes Bearbeitungsreglement, wie in **Art. 4 rVDSG** vorgesehen, zu erstellen. Es ist eher praxisfern, ein solches Reglement für automatisierte Datenbearbeitungsprozesse zu erstellen, welche stetigem Wandel unterliegen und regelmässig angepasst oder erweitert werden. So sind auch die Ausarbeitung und Anpassung eines solchen Reglements in zumindest grösseren Unternehmen nur unter Einbindung verschiedener Funktionen möglich, was mit einem erheblichen Zeit- und Kostenaufwand verbunden wäre. Die Pflicht knüpft an Datenbearbeitungen an, die ein hohes Risiko für den Betroffenen bergen, weil "*umfangreich besonders schützenswerte Personendaten*" bearbeitet werden oder ein "*Profiling mit hohem Risiko*" durchgeführt wird. Im Umkehrschluss muss dies bedeuten, dass dann, wenn gemäss DSFA nach ergriffenen Massnahmen kein hohes Risiko mehr besteht, diese Pflicht entfällt. Das vorgeschlagene Bearbeitungsreglement soll faktisch denselben Inhalt wie das Datenbearbeitungsverzeichnis nach Art. 12 rDSG aufweisen. Da aber jedes Unternehmen, das nicht unter den Ausnahmetatbestand von Art. 12 Abs. 5 rDSG fällt, ohnehin ein Verzeichnis führen muss, ist es unserer Ansicht nach nicht länger notwendig, die Pflicht zur Erstellung eines Bearbeitungsreglements beizubehalten und zu erweitern.

18 Zudem wurde im rDSG bewusst auf allgemeine Dokumentationspflichten, die über die Führung eines Bearbeitungsverzeichnisse hinausgehen, verzichtet. Umso mehr ist es überraschend, dass nun doch zusätzliche Dokumentationspflichten mittels rVDSG für private Datenbearbeiter eingeführt werden sollen. Auch diesbezüglich sind wir der Auffassung, dass die rVDSG zusätzliche Pflichten schaffen würde, die über das rDSG hinausgehen. **Wir regen deshalb an, Art. 4 rVDSG ersatzlos zu streichen**.

19 **Zu den Aufbewahrungspflichten**: Für die verschiedenen neu eingeführten Aufbewahrungspflichten nach **Art. 3 Abs. 4 rVDSG** für die Protokolle, **Art. 18 rVDSG**

für die DSFA, **Art. 19 Abs. 5 rVDSG** für Datenschutzverletzungen und **Art. 20 Abs. 5 rVDSG** für die Verweigerung, Einschränkung oder den Aufschub einer Auskunft gibt es unserer Ansicht nach grundsätzlich keine gesetzliche Grundlage. Vor allem geht die Pflicht, "*alle mit den Vorfällen zusammenhängenden Tatsachen*" im Rahmen einer Datenschutzverletzung zu dokumentieren, sehr weit und scheint vor der Tatsache, dass Art. 19 Abs. 1 rVDSG eine Liste meldepflichtiger Informationen aufzählt, unverhältnismässig. **Wir regen daher an, den zweiten Satz in Art. 19 Abs. 5 ersatzlos zu streichen.**

20 Darüber hinaus variieren die festgelegten Aufbewahrungsfristen zwischen zwei und drei Jahren. Es ist nicht nachvollziehbar, wie diese Fristen festgelegt wurden und weshalb sie nicht einheitlich sind, zumal dadurch auch deren Umsetzung im Unternehmen erschwert wird. **Aus diesem Grund regen wir an, dass, sofern die Aufbewahrungspflichten mangels gesetzlicher Grundlage nicht ersatzlos gestrichen werden, sie zumindest einheitlich festgelegt werden.**

21 **Zur Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten**: Es ist begrüssenswert, dass der Bundesrat in **Art. 26 rVDSG** präzisiert, unter welchen Bedingungen private Datenbearbeiter mit weniger als 250 Mitarbeitenden von der Pflicht zur Führung eines Datenbearbeitungsverzeichnisses ausgenommen sind. Unklar erscheint jedoch, ob diese Liste abschliessend ist, ob damit ein hohes Risiko für die Verletzungen der Persönlichkeit der Betroffenen immer nur dann besteht, wenn umfangreich besonders schützenswerte Daten bearbeitet werden bzw. wenn Profiling mit hohem Risiko durchgeführt wird und ob dies dann auch auf die Durchführung einer DSFA nach Art. 22 rDSG und die Meldepflichten bei Datenschutzverletzungen nach Art. 24 rDSG übertragbar ist, in dem Sinne, dass sonst kein hohes Risikos für die Betroffenen besteht. **Wir regen an, dass der Bundesrat diese Bestimmung dahingehend präzisiert, ob die Liste abschliessend ist und prüft, ob diese Einschätzung auf Art. 22 und 24 rDSG übertragbar ist**.

2 Informationspflichten

22 **Art. 13 und 15 rVDSG** sind so formuliert, als würde den Auftragsbearbeiter auch eine Informationspflicht nach Art. 19 f. rDSG treffen. Dies ist unzutreffend, weil gesetzlich so gar nicht vorgesehen. **Wir regen daher stark an, "*Auftragsbearbeiter*" in Art. 13 und 15 rVDSG ersatzlos zu streichen**.

23 In Anlehnung an die EU DSGVO legt **Art. 13 Abs. 1 rVDSG** fest, dass "*die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form*" mitgeteilt werden muss. Hierzu hält der Erläuternde Bericht fest, dass die Information "*stets auf der ersten Kommunikationsstufe*", wie z.B. bei einem Websitebesucher eine Publikation auf der Internetseite oder in einem "*telefonischen Setting*" eine mündliche Mitteilung (Erläuternder Bericht, S. 30). Zudem steht explizit, dass eine Kommunikation über die Webseite nicht

immer genügen wird (Erläuternder Bericht, S. 30). Dies erscheint unverhältnismässig, unpraktikabel und unnötig erschwerend, insbesondere auch, weil es in der Praxis weit verbreitet ist, die Datenschutzerklärung auf der eigenen Website zu publizieren und in anderen Dokumenten oder "Settings" auf die Website zu verweisen. Je nach Umständen ist es zudem nicht möglich, in gleich umfassender Weise, wie von Art. 19 rDSG verlangt, zu informieren. Namentlich bei einem "*telefonischen Setting*" wird die Information notgedrungen weniger umfassend ausfallen als dies in einer schriftlichen Datenschutzerklärung auf der Website der Fall ist. Insofern liegt es im Interesse des Anrufers, auf die Website verwiesen zu werden.

24 Unserer Ansicht nach ist die Bestimmung in Art. 13 Abs. 1 rVDSG als solche verständlich formuliert, da sie technologieneutral festlegt, dass die Information präzis, verständlich und leicht zugänglich sein muss. Im Zusammenhang mit dem Erläuternden Bericht ergeben sich aber die oben beschriebenen Anwendungsschwierigkeiten, weshalb wir anregen, dass im Erläuternden Bericht klargestellt wird, dass Unternehmen je nach Datenbearbeitungsprozess und Zeitpunkt der Erhebung der Daten unterschiedliche Formen für die Information wählen können, insbesondere auch in einem "*telefonischen Setting*", solange die Information präzis, verständlich und leicht zugänglich ist.

25 **Art. 15 rVDSG** sieht eine Information an Empfänger von Daten betreffend deren Aktualität, Zuverlässigkeit und Vollständigkeit vor. Diese Pflicht wurde aus Art. 12 VDSG übernommen, scheint jedoch unnötig, und zwar, weil jeder Verantwortlicher selber die Pflicht hat, die Richtigkeit der Daten sicherzustellen (Art. 6 Abs. 5 rDSG), und eine allfällige Informationspflicht bei Bekanntgabe von Daten zwischen den beiden Verantwortlichen vertraglich festgelegt werden kann, wenn sie über ihre Pflichten nach Art. 6 rDSG hinausgehen möchten. **Unserer Ansicht nach bedarf es keiner solchen Pflicht, und wir regen deshalb an, diese Pflicht ersatzlos zu streichen.**

26 **Art. 16 rVDSG** beinhaltet eine Pflicht, Empfänger von Personendaten darüber zu informieren, wenn Personendaten berichtigt, gelöscht, vernichtet oder deren Bearbeitung eingeschränkt wird. Diese Pflicht ist an Art. 19 EU DSGVO angelehnt. Jedoch ist darauf hinzuweisen, dass diese Pflicht bereits im Vorentwurf zum rDSG vorgesehen war (Art. 19 lit. b Vorentwurf rDSG), aber nach der Vernehmlassung ersatzlos gestrichen wurde. Es liefe daher dem Willen des Gesetzgebers zuwider, diese Pflicht über die rVDSG dennoch einzuführen. **Wir regen deshalb an, diese Pflicht ersatzlos zu streichen**.

27 **Schliesslich regen wir an, Art. 17 rVDSG ersatzlos zu streichen**, da es nicht Aufgabe des Datenschutzrechts ist, allgemeine Diskriminierungen, die nicht auf eine Datenbearbeitung zurückzuführen sind, zu verbieten.

III Auftragsdatenbearbeitung und Auslanddatentransfers

1 Auftragsdatenbearbeitung

28 Gemäss **Art. 6 Abs. 1 Satz 2** muss "[der Verantwortliche] *sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden*". Wir erachten diese Bestimmung in nachfolgender Hinsicht als unglücklich. Nach vorgeschlagenem Wortlaut verletzt ein Verantwortlicher diese Bestimmung, wenn er mit einem Auftragsbearbeiter einen Vertrag abschliesst, der über die gesetzlichen Anforderungen hinausgeht und diese über das rDSG hinausgehenden Anforderungen beim Auftragsbearbeiter nicht sicherstellt, selbst wenn die Auftragsbearbeitung im Rahmen des Gesetzes erfolgt. Wir regen an, **in Satz 2 "*vertrags- oder*" ersatzlos zu streichen**.

29 **Art. 6 Abs. 2** richtet sich an Bundesorgane und Private. Für uns erschliesst sich nicht, weshalb diese Bestimmung auch für Private gelten soll. Auch der Erläuternde Bericht führt dies nicht weiter aus. Für Private regelt bereits Art. 9 Abs. 1 lit. a rDSG, dass ein Auftragsbearbeiter die Daten nur so bearbeiten darf, wie der Verantwortliche es selbst tun dürfte. Es besteht deshalb kein Bedarf, dies in Art. 6 Abs. 2 zu wiederholen.

30 Überträgt ein Verantwortlicher die Bearbeitung an einen Auftragsbearbeiter im Ausland – in dieser Konstellation findet das rDSG auf den Auftragsbearbeiter keine Anwendung – versteht sich von selbst, dass der Verantwortliche die Regeln von Art. 16-18 rDSG einhalten muss.

31 Soll mit Art. 6 Abs. 2 rVDSG jener Anwendungsfall geregelt werden, in dem ein ausländischer Auftragsbearbeiter Daten bearbeitet, die ihm zuvor nicht aus der Schweiz übermittelt worden sind, wäre dies in Art. 16 rDSG zu regeln und nicht im Rahmen der Auftragsbearbeitung.

32 **Wir regen daher an, Art. 6 Abs. 2 rVDSG ersatzlos zu streichen**.

2 Auslanddatentransfers

33 **Art. 9 Abs. 1 lit. a bis k rVDSG** definiert den Mindestinhalt von Datenschutzklauseln und spezifischen Garantien. Die EU DSGVO enthält keinen vergleichbaren Katalog für Vertragsklauseln (vgl. Art. 46(3) EU DSGVO), sondern regelt nur den Mindestinhalt von verbindlichen internen Datenschutzvorschriften ("**BCRs**").

34 Zudem unterscheiden Art. 9 Abs. 1 lit. a bis k rVDSG nicht danach, ob Daten an einen Verantwortlichen oder an einen Auftragsdatenbearbeiter übermittelt werden. Wie auch die revidierten EU-Standardvertragsklauseln vom 4. Juni 2021, sollte der Mindestinhalt danach unterscheiden. So muss bspw. ein Vertrag, der als Grundlage einer Datenübermittlung von einem Verantwortlichen an einen

Auftragsdatenbearbeiter dient, die Rechte der betroffenen Personen (lit. k) nicht regeln, sondern vorsehen, dass der Auftragsbearbeiter den Verantwortlichen notifizieren soll, wenn Betroffene solche Rechte geltend machen und den Verantwortlichen bei der Bearbeitung der Anfragen unterstützen soll.

35 Wir regen daher an, den Mindestinhalts-Katalog von Art. 9 Abs. 1 lit. a bis k rDSG entweder **ersatzlos zu streichen und in den BCR zu regeln** oder, wenn er beibehalten werden soll, **anzupassen**, um den verschiedenen Datenübermittlungsszenarien gerecht zu werden.

IV Recht auf Datenherausgabe oder -übertragung

36 Zur Konkretisierung des Rechts auf Datenherausgabe und -übertragung verweist **Art. 24 rVDSG** auf bestimmte Absätze von Art. 20, sowie Art. 21, 22 und 23 rVDSG.

37 Dieser pauschale Verweis ist aus unserer Sicht nicht sachgerecht, verfolgt eine betroffene Person mit Ausübung des Rechts auf Datenherausgabe oder -übertragung doch nicht dasselbe Interesse, wie wenn sie ihr Auskunftsrecht ausübt. "Lock In"-Effekten kann nur begegnet werden, wenn betroffene Personen die Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten. Dementsprechend kommt es beim Recht auf Datenherausgabe und -übertragung entscheidend darauf an, dass der Verantwortliche die Daten in einem bestimmten Format herausgibt. Darauf kommt es beim Auskunftsrecht nicht an.

38 Folglich regen wir an, Art. 24 rVDSG so **anzupassen**, dass für Verantwortliche klar wird, was von ihnen verlangt wird, insbesondere ist das Format der herausgegebenen Daten zu konkretisieren.

C Anpassungsvorschläge für einzelne Artikel

Artikel	Bemerkung	Anpassungsvorschlag
1	Implementierungskosten *und* Implementierungsaufwand sind für die Festlegung von organisatorischen und technischen Massnahmen ausschlaggebend.	Präzisierung: Implementierungskosten mit Implementierungsaufwand ersetzen
2	Siehe oben Rz. 7 ff.	Substanzielle Überarbeitung und/oder Präzisierung

Artikel	Bemerkung	Anpassungsvorschlag
3 Abs. 4	Siehe oben Rz. 14-15	Satz 1 "getrennt vom System, in welchem die Personendaten bearbeitet werden" sowie Satz 2 ersatzlos streichen
4	Siehe oben Rz. 17-18	Pflicht zur Führung eines Bearbeitungsreglements ersatzlos streichen; alternativ: kürzen und detaillierte Auflistung, was im Bearbeitungsreglement geregelt sein muss streichen; Vorlage des Bearbeitungsreglements beim internen Datenschutzberater ist in jedem Fall zu streichen, da es im rDSG gar keine Pflicht zur Ernennung eines Datenschutzberaters gibt
Art. 6 Abs. 1 Satz 2	Siehe oben Rz. 28	in Satz 2 "vertrags- oder" ersatzlos streichen.
Art. 6 Abs. 2	Siehe oben Rz. 29 f.	Ersatzlos streichen
Art. 9 Abs. 1 lit. a bis k	Siehe oben Rz. 33 ff.	Ersatzlos streichen oder anpassen.
13	Siehe oben Rz. 22 f.	Erläuternder Bericht anpassen; Auftragsbearbeiter ersatzlos streichen
15	Siehe oben Rz. 25	Ersatzlos streichen

Artikel	Bemerkung	Anpassungsvorschlag
16	Siehe oben Rz. 26	Ersatzlos streichen
17	Unnötige Vorschrift, auch wenn nicht schädlich für private Datenbearbeiter (siehe oben Rz. 27)	Ersatzlos streichen
3 Abs. 4, 18, Art. 19 Abs. 5 und Art. 20 Abs. 5	Siehe oben Rz. 19-20	Ersatzlos streichen; alternativ Aufbewahrungsfristen vereinheitlichen
18	Unklar, ob "*schriftlich*" i.S.v. Art. 13 OR gemeint ist	Präzisieren, dass Textform gemeint ist und nicht Schriftlichkeit nach Art. 13 OR
19 Abs. 5	Siehe oben Rz. 19-20	Zweiter Satz ersatzlos streichen; alternativ Präzisierung, dass nicht mehr als in Art. 19 Abs. 1 lit. a-g rVDSG aufgelistet ist, dokumentiert werden muss
20 Abs. 3	Unklar, was mit "muss für die betroffene Person "*verständlich*" sein" gemeint ist und ob das bedeutet, dass ein Datenbearbeiter allenfalls mehr Informationen geben muss, als gemäss Auskunftsrecht notwendig ist	Präzisieren, dass nicht mehr Informationen als in Art. 25 Abs. 1 und 2 rDSG aufgelistet sind, erteilt werden müssen
21 Abs. 1	Bei gemeinsamer Verantwortlichkeit sollte es möglich sein, stellvertretend Auskunft zu erteilen, sofern die Personendaten betroffen sind, für die sie gemeinsam verantwortlich	Präzisieren, "Sind für die Bearbeitung von Personendaten mehrere *gemeinsam* verantwortlich […]"

Artikel	Bemerkung	Anpassungsvorschlag
	sind (vertraglich kann dies natürlich anders geregelt werden, aber dies ist Sache der gemeinsamen Verantwortlichen)	Art. 21 Abs. 1 zweiter Satz ersatzlos streichen
Art. 24	Siehe oben Rz. 36 ff.	Präzisierung
Art. 25	Dieser Artikel nimmt die Schulungs- und Beratungsfunktion nach Art. 10 Abs. 2 lit. a rDSG nicht auf.	Präzisierung, ob Aufgaben abschliessend aufgezählt sind oder nicht
Art. 26	Siehe oben Rz. 21	Präzisierung

* * * * *

Zusammenfassend erachten wir die vorgeschlagene Revision der Verordnung zum Bundesgesetz über den Datenschutz in den von uns vertieft besprochenen vier Kernpunkten als verbesserungswürdig und regen an, unsere Anpassungsvorschläge bei der Überarbeitung des Entwurfs zu berücksichtigen.

Für Ihre allfälligen Rückfragen stehen wir gerne zur Verfügung.

Freundliche Grüsse

Dr. Corrado Rampini

Dr. Jan Kleiner

Dr. Rehana Harasgama

Dr. Christian Kunz

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

Der Generalsekretär
CH - 1000 Lausanne 14
Tel. 021 318 91 02
Fax 021 323 37 00
Korrespondenznummer 003.1_2021

An die Vorsteherin des Eidgenössischen
Departements für Justiz und Polizei EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

per E-Mail an:
jonas.amstutz@bj.admin.ch

Lausanne, 12. Oktober 2021/run

Ämterkonsultation: Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin

Mit Brief vom 23. Juni 2021 haben Sie das Bundesgericht eingeladen, in oben erwähnter Ämterkonsultation Stellung zu nehmen; dafür danken wir Ihnen bestens.

Wir teilen Ihnen mit, dass das Bundesgericht auf eine Stellungnahme verzichtet.

Genehmigen Sie, sehr geehrte Frau Bundesrätin, den Ausdruck unserer ausgezeichneten Hochschätzung.

Freundliche Grüsse
Paul Tschümperlin

Kopie
- Bundesstrafgericht
- Bundesverwaltungsgericht
- Bundespatentgericht

biblio}suisse

Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
CH-3003 Bern
Per Mail:
jonas.amstutz@bj.admin.ch

Aarau, 7. Oktober 2021

Vernehmlassung von Bibliosuisse zur
Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrter Herr Amstutz

Wir nützen die Gelegenheit zur Stellungnahme im Rahmen des Vernehmlassungsverfahrens zur Verordnung zum Bundesgesetz über den Datenschutz wie folgt:

1.1

Für die Bibliotheken und deren Library Management Systeme (LMS) halten wir fest, dass diese Personendaten in Verbindung mit der registrierten Nutzung von Medien im Rahmen von Ausleihen keinesfalls unter die Bestimmungen von Art. 4 Ziff. 1 E-VDSG fallen können. Diese Feststellung gilt sowohl für die Bibliotheken also auch die LMS-Dienstleister als «Auftragsbearbeiter» im Sinn der Verordnung. Es handelt sich dabei nicht um «umfangreich bearbeitete besonders schützenswerte Personendaten» gemäss Art. 5 Bst.c nDSG und den Erläuterungen in der Botschaft des Bundesrates zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (17.059). Als besonders schützenswerte Personendaten werden dort aufgeführt: ethnische Herkunft, Rassenzugehörigkeit, Gesundheitsdaten, Intimsphäre, Sexualleben, Geschlechtsidentität, genetische und biometrische Daten.

1.2

Das Gesetz selber listet zum Terminus explizit die folgenden Inhalte auf: Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten, biometrische Daten, die eine natürliche Person eindeutig identifizieren, Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, Daten über Massnahmen der sozialen Hilfe. Diese Aufzählung ist abschliessend und nicht beispielhaft, weshalb die von Bibliotheken erhobenen

Daten davon ausgeschlossen werden können. Ausgeliehene Medien können zwar Hinweise über die Interessen von Personen geben; es sind aber keine Daten die «Ansichten oder Tätigkeiten» dokumentieren, wie das im Gesetz spezifiziert wird. Darum können Ausleihdaten nicht als besonders schützenswerte Personendaten interpretiert werden.

1.3

Ebenso wenig sind die LMS-Datenbanken geeignet, «ein Profiling mit hohem Risiko» zu ermöglichen, wie das in den Materialien zum nDSG und zur E-VDSG erläutert wird. Dieses Verständnis ist für uns von Bedeutung, weil damit die Pflicht von Art. 4 E-VDSG zur Erstellung eines Bearbeitungsreglements entfällt. Summa summarum fallen unter den beiden Aspekten «besonders schützenswerte Personendaten» sowie «Profiling mit hohem Risiko» die Bibliotheken und deren LMS-Daten bzw. ihre Auftragsbearbeiter nicht unter die Bestimmung von Artikel 4 der E-VDSG.

2.

Analog ist eine Pflicht der Bibliotheken gemäss Art. 26 E-VDSG zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten zu verneinen. Die beiden Buchstaben a und b sehen eine Ausdehnung auch auf Unternehmen und privatrechtliche Organisationen mit weniger als 250 Beschäftigten vor. Die genannten Voraussetzungen «umfangreich besonders schützenswerte Personendaten» oder «Profiling mit hohem Risiko» werden von LMS-Datenbanken gemäss den Ausführungen oben nicht erfüllt.

3.

Wir möchten sicherstellen, dass unsere Interpretation von nDSG und E-VDSG gemäss den vorstehenden Ausführungen zutrifft. Deshalb beantragen wir, dass die Verordnung in diesem Sinn ergänzt und verdeutlicht wird. Wir schlagen vor, Art. 4 durch einen neuen Absatz 2 zu ergänzen und die weiteren Absätze entsprechen neu zu nummerieren:

4.

VDSG, Artikel 4, neuer Absatz 2:

«Nicht unter die vorstehenden Buchstaben a und b fallen Daten, die von Bibliotheken, Mediotheken, vergleichbaren Einrichtungen und ihren Auftragsbearbeitern für Medienausleihen erhoben werden.»

5.

Die Nummerierung der folgenden Absätze ist entsprechend anzupassen.

Wir danken Ihnen für die Kenntnisnahme unserer Vernehmlassung und der entsprechenden Bearbeitung der künftigen Verordnung.

Mit freundlichen Grüssen

Hans Ambühl, Rechtsanwalt
Präsident Bibliosuisse

Dr. iur. Hans Ulrich Locher
Geschäftsführer Bibliosuisse

Bundesstrafgericht
Tribunal pénal fédéral
Tribunale penale federale
Tribunal penal federal

Verwaltungskommission
Viale Stefano Franscini 7
CH-6500 Bellinzona
Tel. +41 58 480 68 68
Fax +41 58 480 68 42
info@bstger.ch

Registratur Nummer: 1.1.1.8

An die Vorsteherin des Eidgenössischen
Departements für Justiz und Polizei EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

per E-Mail an:
jonas.amstutz@bj.admin.ch

Bellinzona, 12. Oktober 2021/BOM

Vernehmlassungsverfahren
Entwurf zur Totalrevision der Verordnung zum BG über den Datenschutz

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 23. Juni 2021 haben Sie das Bundesstrafgericht eingeladen, im oben erwähnten Vernehmlassungsverfahren Stellung zu nehmen; dafür danken wir Ihnen bestens.

Wir teilen Ihnen mit, dass das Bundesstrafgericht auf eine Stellungnahme verzichtet.

Genehmigen Sie, sehr geehrte Frau Bundesrätin, den Ausdruck unserer ausgezeichneten Hochschätzung.

Sylvia Frei
Präsidentin

BUNDESSTRAFGERICHT
BELLINZONA

Marc-Antoine Borel
Generalsekretär

Kopie an
- Bundesgericht
- Bundesverwaltungsgericht
- Bundespatentgericht

Bundesverwaltungsgericht
Tribunal administratif fédéral
Tribunale amministrativo federale
Tribunal administrativ federal

La Conférence des présidents

Case postale
CH-9023 St-Gall
Telephone +41 58 465 27 27
Numero de classement: 024.1
Numéro d'objet: 2021-200

Département fédéral de justice et police
Madame la conseillère fédérale
Karin Keller-Sutter
Palais fédéral ouest
CH-3003 Berne

version PDF et version Word par voie électronique à l'adresse suivante :

jonas.amstutz@bj.admin.ch

St-Gall, 12 octobre 2021 / hah

Procédure de consultation: Révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Madame la conseillère fédérale,
Madame, Monsieur,

Nous vous remercions de l'opportunité donnée au Tribunal administratif fédéral de prendre position sur la révision de l'ordonnance citée. Nous avons pris note avec intérêt du projet et nous avons le plaisir de vous faire part des remarques suivantes :

1.1.1 Evaluation du niveau de protection adéquat des données personnelles d'un état étranger ou d'un organisme international (ad art. 8 P-OLPD)

Sur la base de l'art. 16 al. 1 nLPD, le Conseil fédéral constate que l'Etat étranger dispose d'une législation assurant un niveau de protection adéquat ou qu'un organisme international garantit un niveau de protection adéquat. Le résultat de cet examen est publié sous la forme d'une ordonnance du Conseil fédéral. L'art. 8 al. 4 P-OLPD, tout comme l'art. 16 al. 2 nLPD d'ailleurs, se réfère toutefois à la notion de décision. L'on peut cependant s'interroger quant à savoir s'il s'agit bien là d'une décision au sens de l'art. 5 PA. Le Tribunal tient à le souligner.

1.1.2 Clauses types de protection des données (ad art. 10 P-OLPD)

En l'absence de constatation au sens de l'art. 16 al. 1 nLPD, des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti, par exemple par des clauses type de protection des données préalablement approuvées, établies ou reconnues par le PFPDT (art. 16 al. 2 let. d nLPD). Selon le rapport explicatif, le PFPDT rend une décision au sens de l'art. 5 PA.

En principe une décision fixe un régime juridique individuel et concret et s'oppose en cela à la norme qui est de nature générale et abstraite. La décision est individuelle dans la mesure où elle s'adresse à un cercle déterminé de destinataires et concrète dans la mesure où elle se rattache à une situation particulière (cf. MOOR/POLTIER, Droit administratif, Vol. II, 3e éd., 2011, p. 198 ; MOSER/BEUSCH/KNEUBÜHLER, Prozessieren vor dem Bundesverwaltungsgericht, 2e éd., 2013, nº 2.12 ss).

En l'occurrence, il n'est pas certain que la publication, par le PFPDT, de clauses types de protection des données au sens de l'art. 10 P-OLPD puisse revêtir la forme d'une décision susceptible de recours au sens de l'art. 5 al. 1 PA, en particulier lorsque le PFPDT les établit, d'office, en l'absence de toute requête expresse d'un administré. En effet, à première vue, la publication de clauses types ne crée, ne modifie ou n'annule pas des droits et des obligations pour un particulier et ne vise pas à s'appliquer à un cas d'espèce. Elle semble bien plutôt revêtir la forme d'une recommandation générale et abstraite qui assure aux particuliers qu'une communication de données reposant sur l'une des clauses types satisfait aux prescriptions légales. Il leur appartient encore de faire reposer, dans les faits, leurs communications sur une telle clause. A noter que les particuliers demeurent libres de recourir à un autre instrument prévu par l'art. 16 al. 2 nLPD, notamment aux clauses de protection et garanties spécifiques – lesquelles sont d'ailleurs soumises uniquement à déclaration et non pas à autorisation, ce qui tendrait à confirmer que le législateur n'a pas souhaité que soit rendue une décision au sens de l'art. 5 PA à ce stade. La vérification de la conformité de la communication avec les règles sur la protection des données devrait s'effectuer *ex post*, dans le cadre d'une enquête menée par le PFPDT et qui aboutirait bien, là et là seulement, à une décision susceptible de recours (art. 52 nLPD).

1.1.3 Règles d'entreprise contraignantes (ad art. 11 P-OLPD)

Les règles d'entreprise contraignantes s'appliquent à toutes les entreprises d'un même groupe et doivent être respectées par celles-ci. Ces règles portent non seulement sur les points mentionnés à l'art. 9 al. 1 P-OLPD, mais aussi sur la structure et les coordonnées du groupe d'entreprises et de chacune de ses entités, ainsi que sur les mécanismes mis en place au sein des groupes d'entreprises pour garantir que ces règles d'entreprises soient effectivement respectées. Là encore, selon le rapport explicatif, le PFPDT rendrait une décision au sens de l'art. 5 PA.

On se trouverait certes davantage ici dans un cas individuel et concret. Toutefois, la problématique exposée ci-dessus resterait la même. En effet, les entreprises n'ont pas l'obligation de soumettre à l'approbation du PFPDT des règles d'entreprise contraignantes. Elles peuvent avoir recours à d'autres garanties comme des clauses types ou des clauses individuelles soumises uniquement à déclaration. Il suit de là que le contrôle, dans un cas particulier, par le PFPDT, des règles d'une entreprise ou d'un groupe d'entreprises devrait davantage revêtir la forme d'un renseignement ou d'une assurance fournie par l'administration, à l'instar d'un ruling, et qui lierait cette dernière aux conditions fixées par la jurisprudence. Dans cette hypothèse, il s'agirait ensuite de vérifier, dans le cadre d'une enquête *ex post*, si l'entreprise pouvait de bonne foi se référer aux renseignements fournis par le PFPDT.

En effet, c'est dans un second temps, lorsque le PFPDT ouvre une enquête concernant des violations de prescriptions de protection des données que la question de savoir si l'entreprise a respecté ou non les prescriptions de l'art. 16 nLPD doit se poser. Le choix de la mesure (clause individuelle, clause type ou règle d'entreprise) reste de la responsabilité individuelle des particuliers. Ce n'est qu'a l'issue de cette enquête qu'une décision au sens de l'art. 5 PA devrait alors être rendue.

1.1.4 Conclusions

Il nous paraît impératif de prendre en considération que le rôle du TAF ne doit pas être celui d'une autorité de contrôle *ex ante* des mesures prises par les particuliers pour se conformer aux prescriptions en matière de protection des données et de communication des données à l'étranger. Outre les problèmes de ressources que cela poserait pour le Tribunal, et plus particulièrement pour la Chambre 1 de la Cour I, la nLPD ne prévoit aucunement que la publication des clauses types ou l'examen des règles d'entreprise fasse l'objet d'une décision formelle sujette à recours.

Il en va, en réalité, de même du projet d'ordonnance qui ne contient aucune prescription en ce sens. C'est le rapport explicatif du Conseil fédéral qui parle pour la première fois de décision au sens de l'art. 5 PA à ce stade déjà.

Or, comme considéré, le rôle du TAF devrait être uniquement celui de vérifier *ex post* le résultat de la procédure d'enquête menée par le PFPDT en cas de violation des dispositions sur la protection des données (cf. art. 52 nLPD). Ce n'est que dans ce cadre-là que l'autorité de recours devrait exercer son contrôle. Elle ne devrait pas intervenir lorsque le PFPDT publiera sur son site internet des clauses types ou qu'il vérifiera *ex ante* le contenu des règles d'une entreprise avant toute communication effective.

Pour le reste, le Tribunal ne voit pas d'autres points qui seraient susceptibles d'impacter son fonctionnement, le nombre de procédures ou l'allocation des ressources au sein de la Cour I. Nous n'avons donc pas d'autres remarques particulières à formuler sur le projet mis en consultation.

En vous remerciant de l'attention portée à ces lignes, nous vous prions d'agréer, Madame la Conseillère fédérale, Madame, Monsieur, l'expression de notre parfaite considération.

Le Président de la
Conférence des présidents

David Weiss

TRIBUNAL ADMINISTRATIF FÉDÉRAL
SUISSE

Le Secrétaire général suppl.

Bernhard Fasel

Copie à

- Tribunal fédéral
- Tribunal pénal fédéral
- Tribunal fédéral des brevets

Centre Patronal

Madame la Conseillère fédérale
Karin Keller-Sutter
Cheffe du Département fédéral
de justice et police
Palais fédéral ouest
3003 Berne

jonas.amstutz@bj.admin.ch

Paudex, le 13 octobre 2021
SHR

Consultation fédérale – révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Madame la Conseillère fédérale,

Nous avons pris connaissance de la consultation mentionnée sous rubrique et nous permettons de vous transmettre ci-après notre prise de position.

I. Contexte

Après plus de deux ans de discussions et une procédure de conciliation entre les deux Chambres, la révision totale de la loi fédérale sur la protection des données a été adoptée le 25 septembre 2020. Les débats ont montré la difficulté qu'il y a à trouver des solutions qui protègent les citoyens et leurs données, mais ne pénalisent pas les entreprises dans leurs activités. La loi va moins loin que le Règlement européen (RGPD) mais demandera un important travail d'adaptation aux entreprises. Son entrée en vigueur, préalablement annoncée pour début 2022, devrait être repoussée à fin 2022, voire début 2023. Si cela laisse un délai supplémentaire pour s'adapter, il demeure toutefois que les entreprises doivent s'y prendre suffisamment tôt, le processus d'adaptation aux nouvelles exigences légales pouvant prendre plusieurs mois. Il s'agira pour elles d'identifier les potentielles activités de traitement concernées, d'analyser le statut actuel de l'entreprise et d'identifier les écarts de conformité avec le nouveau droit, d'établir un plan d'action pour mettre en place les nouvelles dispositions légales et notamment les registres des actions de traitement et de contrôler ensuite que la mise en place des outils a bien été faite. Les entreprises qui respectent déjà le RGPD seront avantagées dans ce processus.

Les nouvelles règles en matière de protection des données sont incontournables et les entreprises n'auront d'autre choix que de s'adapter et de s'y conformer. C'est toutefois aussi une occasion pour les entreprises de revoir leurs processus et leurs méthodes pour optimiser le fonctionnement de leur organisation, et cela au-delà des fonctions purement informatiques. Faut-il voir dans cette évolution un frein à la numérisation et à l'innovation en matière d'utilisation des données? En réalité, il s'agit plutôt d'une condition pour que la numérisation et l'innovation soient acceptées par les individus. La collecte de données et leur traitement plus ou moins complexe restent possibles si les personnes concernées sont correctement informées, qu'elles comprennent l'utilité des processus de traitement et qu'elles se laissent convaincre de donner leur consentement. Un effort de persuasion est nécessaire, mais il sera payant en termes de transparence et de confiance.

Route du Lac 2
1094 Paudex
Case postale 1215
1001 Lausanne
T +41 58 796 33 00
F +41 58 796 33 11
info@centrepatronal.ch

Kapellenstrasse 14
Postfach
3001 Bern
T +41 58 796 99 09
F +41 58 796 99 03
cpbern@centrepatronal.ch

www.centrepatronal.ch

II. Le projet d'OLPD

Le 23 juin dernier, le Conseil fédéral a mis en consultation le projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD). L'objectif de l'OLPD est de préciser les principes fixés dans la LPD et de fixer des règles de mise en œuvre.

De manière générale, nous ne sommes pas opposés au projet d'OLPD du Conseil fédéral. Nous partageons la vision suivie qui privilégie une approche fondée sur le risque – plus les droits de la personnalité et les droits fondamentaux de l'individu sont menacés, plus les exigences sont élevées – et qui renonce à fixer des exigences minimales générales applicables à chaque branche. Le projet d'OLPD contient surtout des lignes directrices permettant de déterminer les mesures à prendre. Il incombera ainsi en premier lieu au responsable du traitement de déterminer les mesures nécessaires dans un cas précis, et de les prendre.

Nous relevons encore que là où il existe une marge de manœuvre, le Conseil fédéral doit privilégier les solutions pragmatiques et les moins formalistes, ceci pour garantir la flexibilité nécessaire pour couvrir le large éventail de cas et éviter un excès de réglementation, en particulier pour les entreprises dont les traitements de données sont rares et présentent peu de risques. S'agissant des coûts de mise en œuvre comme critère d'appréciation des mesures techniques et organisationnelles, il convient de privilégier celui de l'économicité des mesures. Ainsi, lorsqu'il existe plusieurs mesures possibles pour garantir un niveau de protection adéquat en toutes circonstances, la variante la plus économique doit pouvoir être privilégiée.

Enfin, pour les entreprises et pour les associations, la mise en pratique de la nouvelle LPD suscite encore beaucoup de questions et il est souhaitable que les autorités fournissent rapidement des guides pratiques, des exemples et des modèles.

Nous relevons encore quelques points particuliers :

- Formalisme excessif et base légale

Nous avons relevé dans plusieurs articles du projet d'OLPD que le texte de l'ordonnance va plus loin que la nouvelle LPD. L'administration fédérale va ici au-delà du mandat qui lui a été donné de mettre en œuvre la LPD. Ceci est contraire au principe de la légalité, une ordonnance ne devant que préciser la loi et en aucun cas introduire de nouvelles obligations légales par la petite porte.

Il s'agit par exemple des articles concernant la sous-traitance (art. 6 OLPD) ou les règles d'entreprises contraignantes où l'ordonnance demande curieusement de communiquer sur la structure du groupe alors que la loi ne le prévoit pas (art. 11 OLPD).

Il découle de ce qui précède que le projet doit être modifié pour respecter la volonté du Parlement (rappelons que le débat avait été long et difficile aux Chambres) et pour respecter le texte de la LPD.

Par ailleurs, certaines exigences sont démesurées et beaucoup trop formalistes. Il en est ainsi de l'art. 15 OLPD relatif aux informations à donner lors de la communication des données personnelles. Les exigences faites aux responsables de données sont telles que toute communication normale et raisonnable à des tiers – et ceci même dans les cas où il n'y aurait aucun risque perceptible – rendraient les opérations quotidiennes et autres moyens de communication usuels beaucoup trop complexes.

Comme nous l'avons développé ci-dessus, le Conseil fédéral doit privilégier les solutions pragmatiques et les moins formalistes, ceci pour garantir la flexibilité nécessaire pour couvrir le large éventail de cas et éviter un excès de réglementation. Le projet d'OLPD doit dès lors être corrigé dans ce sens.

- *Exception pour les petites et moyennes entreprises (PME) – art. 26 OLPD et 12 al. 5 LPD*

Conformément à l'art. 12 al. 5 LPD, l'art. 26 OLPD prévoit une exception à l'obligation de tenir un registre des activités de traitement pour les PME. Ainsi, les entreprises et autres organismes de droit privé, de même que les personnes physiques, employant moins de 250 collaborateurs sont déliés de leur obligation de tenir un registre des activités de traitement à moins que le traitement ne porte sur des données sensibles à grande échelle ou que le traitement constitue un profilage à risque élevé.

Cette exception nous paraît judicieuse, la limite des 250 collaborateurs s'inspirant de ce qui se fait en droit de la société anonyme (SA), par exemple pour les exceptions au contrôle ordinaire (art. 727 al. 2 ch. 2 CO). La grande majorité des PME devraient ainsi bénéficier de cette exception et ne devraient donc pas être tenues par la loi de tenir un registre des activités de traitements ordinaires. Cela est ainsi conforme à l'approche fondée sur le risque privilégiée par le Conseil fédéral.

- *Profilage et profilage à risque élevé*

Savoir s'il fallait inclure le "profilage à risque élevé" dans la loi, à côté du profilage "ordinaire", a été la question la plus controversée et la plus largement débattue de toute la procédure législative. Pour finir, les Chambres fédérales ont suivi les propositions de la conférence de conciliation, selon lesquelles le profilage à risque élevé devrait être défini et spécifiquement réglementé par la loi. Ainsi, dans le cas du profilage à risque élevé, tout consentement éventuellement requis devra être explicitement donné. En outre, les responsables du traitement des données pour l'évaluation des risques de crédit ne pourront plus s'appuyer sur un intérêt légitime et ne pourront donc plus justifier une violation du droit à la vie privée si ladite évaluation du risque de crédit implique un profilage à risque élevé.

La définition juridique de la LPD est très ouverte et une différenciation du profilage "ordinaire" ne sera pas facile en pratique. L'OLPD n'apporte que peu de précisions à ce sujet et il est ici souhaitable que les autorités fournissent rapidement des guides pratiques et des exemples.

- *Conseiller à la protection des données dans l'administration fédérale – art. 27 OLPD*

Le projet prévoit, à son art. 27 OLPD, que « *Tout organe fédéral désigne un conseiller à la protection des données personnelles* ».

Cela signifierait que chaque office désignerait un conseiller, ce qui est totalement disproportionné et entraînerait des surcoûts non justifiés. Cette disposition doit être corrigée et il convient de s'en tenir à la formulation actuelle de l'ordonnance (art. 23 OLPD actuelle), à savoir que « la Chancellerie fédérale et chaque département désignent respectivement et au minimum un conseiller à la protection des données ».

- *Emoluments – art. 45 OLPD*

Nous relevons que l'art. 45 OLPD prévoit à son al. 1 que « *l'émolument perçu par le PFPDT se calcule en fonction du temps consacré* » et que selon son al. 2, « *il varie entre 150 et 350 francs de l'heure [et qu'] il dépend de la complexité de l'affaire et de la fonction de la personne chargée de la traiter* ».

Cette formulation est surprenante et inadéquate. Il ne nous paraît pas acceptable que l'Etat puisse facturer, sans prévoir de limite, des honoraires pour ses tâches de service public et que le justiciable ne sache pas quels seront les émoluments perçus. Ce point doit être corrigé et la fixation d'émoluments sous forme de forfaits, comme le prévoient d'autres ordonnances (par exemple l'OEmol-LTr, RS 822.117), nous paraîtrait appropriée.

III. Conclusions

Au vu de ce qui précède, nous ne sommes pas opposés au projet d'OLPD du Conseil fédéral mais certains points doivent être corrigés. En particulier, nous relevons encore que, là où il existe une marge de manœuvre, le Conseil fédéral doit privilégier les solutions pragmatiques et les moins formalistes. Par ailleurs, certaines dispositions dépassent le cadre d'une ordonnance d'application et doivent être supprimées. L'administration fédérale ne saurait en effet introduire de nouvelles exigences qui ne seraient pas prévues dans la loi et qui vont au-delà des choix faits par le Parlement. Enfin, pour les entreprises et pour les associations, la mise en pratique de la nouvelle LPD suscite encore beaucoup de questions et il est souhaitable que les autorités fournissent rapidement des guides pratiques, des exemples et des modèles.

* * *

En vous remerciant de l'attention que vous porterez à la présente prise de position, nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre haute considération.

Centre Patronal

Sandrine Hanhardt Redondo

Classtime

Input Vernehmlassung zur Revision der Datenschutzverordnung

Datum: 14.10.2021
Autor: Classtime AG, Jan Rihak, jan@classtime.com

Tabellarische Auflistung der Anmerkungen je Artikel E-VDSG

Bemerkung: Punktuell wird mit dem Hinweise "Whitepaper" auf das folgende Dokument verwiesen: "Swiss EdTech Collider_EDK_EDUCA_EdTech Whitepaper_09.2021_Signed.pdf", diesem Input-Dokument beiliegend

Kapitel E-VDSG	**Input Classtime AG**
Art. 1 Grundsätze	Aus unserer Sicht sollte auch der Nutzen der Datenbearbeitung ergänzt werden, im Kontext des Anwendungsfalles: Beispiel: "Welchen Nutzen haben Lehrpersonen, wenn Sie Einsicht haben in Lernstände einzelner Schüler, welche ein Anbieter den Nutzern zur Verfügung stellt?"
Art. 2: Schutzziele	Schutzziele (bzw. deren Angemessenheit) sind in Bezug und im Kontext von Sensitivitätsklassen (siehe Whitepaper) zu beurteilen
Neuer Artikel 3: Nutzen	Die Datenbearbeitung hat im Rahmen einem belegbaren und dokumentierten Nutzen für das Datensubjekt bzw. weiteren Stakeholdern zu erfolgen. Falls das Datensubjekt selber keinen direkten Nutzen aus der Datenbearbeitung zieht, muss der Nutzen für weitere Stakeholder umso besser begründbar sein und im weiteren Kontext wertstiftend sein
Art. 3: Protokollierung	Die Protokollierung ist nach Verhältnismässigkeit zu beurteilen, insbesondere auch im Kontext der Sensitivität der Datenbearbeitung (Vergleich: Whitepaper). Die Trennung und separate Aufbewahrung ist aus unserer Sicht in vielen Fällen nicht verhältnismässig, wird in Realität so kaum umgesetzt, und wäre innovationshemmend falls erzwungen/durchgesetzt.
Art. 4:	Keine Anmerkungen.
Art. 5:	Keine Anmerkungen.
Art. 6:	Keine Anmerkungen.
Art. 7:	Keine Anmerkungen.

Art. 8:	Die Beurteilung der Angemessenheit der Weitergabe von Personendaten ins Ausland ist vor allem auch im Kontext der Nutzung von ausländischen Drittdienstleistern zu beurteilen. Die faktische Nulltoleranz ggü. US-Anbietern trägt der Realität kaum Rechnung (zum Beispiel: Nutzung von Microsoft Produkten ist weit verbreitet, obschon bei Microsoft in wesentlichem Umfang Drittdienstleister in den USA eingesetzt werden, und zwar für hoch-sensitive Elemente wie Dateiablagen / Cloud-Storage. Obwohl rechtlich verboten, werden solche Verbote für die klassischen Tech-Giganten, z.B. Microsoft, kaum durchgesetzt. Hier dürfen kleinere CH-Anbieter, welche Drittdienstleiter als Unterauftragnehmer bspw. in den USA nutzen, nicht benachteiligt werden). Die Weitergabe von Personendaten zur Bearbeitung durch Drittdienstleister ist wesentlich zu flexibilisieren, um diese de facto überhaupt durchsetzbar zu halten, und nach Sensitivitätsklassen zu beurteilen (siehe Whitepaper). Die Konsultation von Behörden und ein Abwarten derer Einschätzung führt de facto zu Wettbewerbsnachteilen für kleinere Anbieter (Beispiel: Einsatz von Microsoft Produkten wird nicht in Frage gestellt, auch wenn diese gemäss neusten Richtlinien (Schrems II, welche durch privatim auf CH angewendet werden) nicht mehr freigegeben sind oder wären. CH Anbieter werden jedoch benachteiligt und vom Wettbewerb ausgeschlossen (Classtime AG hat dokumentierte Fälle - US Tech-Giants wie Micorosft werden von behördlichen Einrichtungen weiterhin de-facto gutgeheissen, obwohl diese die Anforderungen nicht erfüllen). Selbstregulierung sollte geprüft werden (siehe Whitepaper).
Art. 9	Zu ergänzen: Der zu erzielende Nutzen der Datenbearbeitung ist ebenfalls zu regeln und zu dokumentieren.
Art. 10	Keine Anmerkungen.
Art. 11	Datenschutzvorschriften sollen ebenfalls für alle in direktem Auftragsverhältnis stehenden Dienstleister gelten (z.B. Berater, Contractor, Freelancer, Entwickler, Agencies).
Art. 12	Kontrolle durch Behörden sollte in der Umsetzung überdacht werden (-> Selbstregulierung, siehe Whitepaper). Anwendung des Artikels 12 ist in Bezug auf Sensitivitätsklassen zu setzen (Verhältnismässigkeit).
Art. 13	Keine Anmerkungen.
Art. 14	Keine Anmerkungen.
Art. 15	Keine Anmerkungen.
Art. 16	Keine Anmerkungen.

Art. 17	Keine Anmerkungen.
Art. 18	Anwendung des Artikels 18 ist in Bezug auf Sensitivitätsklassen zu setzen (Verhältnismässigkeit).
Art. 19	Keine Anmerkungen.
Art. 20	Keine Anmerkungen.
Art. 21	Keine Anmerkungen.
Art. 22	Keine Anmerkungen.
Art. 23	Keine Anmerkungen.
Art. 24	Keine Anmerkungen.
Art. 25	Keine Anmerkungen.
Art. 26	Keine Anmerkungen.
Art. 27	Keine Anmerkungen.
Art. 28	Ergänzung zu den Aufgaben der Datenschutzberaterin / des Datenschutzberaters: Die Prüfung der Bearbeitung von Personendaten muss im Kontext der Anwendungsfälle / des Nutzens der Bearbeitung sowie der Sensitivität getroffen werden (siehe Sensitivitätsklassen und Anforderungen im Whitepaper).
Art. 29	Keine Anmerkungen.
Art. 30	Keine Anmerkungen.
Art. 31	Keine Anmerkungen.
Art. 32	Keine Anmerkungen.
Abschnitt 3 - Pilotversuche	Pilotversuche sollten auch für private Anbieter möglich sein (siehe Vorschlag “Sandbox” im Whitepaper), mit wesentlich tieferen Vorgaben, sofern gewisse Kriterien erfüllt sind (Sandbox-Kriterien).
Art. 33	Keine Anmerkungen.
Art. 34	Keine Anmerkungen.
Art. 35	Keine Anmerkungen.
Art. 36	Keine Anmerkungen.
Art. 37	Keine Anmerkungen.
Art. 38	Keine Anmerkungen.
Art. 39	Keine Anmerkungen.

Art. 40	Keine Anmerkungen.
Art. 41	Anmerkung: Selbstkontrolle sollte im Rahmen von Selbstregulierungsprinzipien auch von privaten Anbietern sowie von behördlichen Einrichtungen (zum Beispiel Schulen) im Rahmen der Selbstregulierungsorganisation (siehe Whitepaper). ebenfalls abverlangt werden.
Art. 42	Keine Anmerkungen.
Art. 43	Keine Anmerkungen.
Art. 44	Keine Anmerkungen.
Art. 45	Keine Anmerkungen.
Art. 46	Keine Anmerkungen.
Art. 47	Keine Anmerkungen.
Art. 48	Keine Anmerkungen.

Generelle Anmerkungen

Anregungen Whitepaper

Wir möchten die Prüfung der Hauptvorschläge des angehängten Whitepapers motivieren, namentlich:

- **Schaffung von Sensitivitätsklassen** für unterschiedliche Anwendungsfälle der Datennutzung
- **Abstufung der Anforderungen für die beteiligten Akteure** (beispielsweise Anbieter) je nach zutreffender Sensitivitätsklasse
- Einführung von **Selbstregulierungsprinzipien**
- Schaffung einer **Sandbox** für Bildungsanbieter, sofern bestimmte Kriterien erfüllt sind
- Stärkere Berücksichtigung von Argumenten der **Datennutzung**, und Definition von Regeln nach welchen Use-Cases zur Datennutzung zu beurteilen sind

Definition “Personendaten” und deren Sensitivität

Die Sensitivität der Personendaten ist im Kontext der Anwendung zu betrachten. Die Anforderung, dass ein Personendatum nicht in einem Drittstaat bearbeitet werden darf, ist losgelöst vom Kontext der Nutzung und allfälliger verknüpfter weitere Datenfelder nicht zielführend und der Sache nicht dienend.

Pseudonymisierung

Ein Pseudonym gilt heute als Personendatum, sofern der Schlüssel noch vorhanden ist. Wenn fortlaufend im Betrieb pseudonymisiert werden muss, kann der Schlüssel nicht weggeworfen werden. Solche Pseudonyme als Personendaten mit den gleichen Restriktionen zu behandeln, obschon aus den Pseudonymen rückwärts nicht auf das Personendatum geschlossen werden kann, ist nicht sinnvoll, wird aber heute von den Behörden so ausgelegt. Es gilt auch hier, dass sich Technologieriesen stillschweigend darüber hinwegsetzen, und dies stillschweigend akzeptiert wird - Jungunternehmen hingegen laufen bei solchen Beurteilungen gegen eine Mauer.

Whitepaper: Data protection and data usage for the Swiss education system 2021+

Outline of a concept for universally applicable data privacy and data usage standards for the education system in Switzerland.

Initial version: 17.10.2020 | Last update: 01.09.2021

Table of Contents

Motivation and goals

The ideas and points mentioned in this document emerged from experiences of certain inconsistencies in requirements and process, loss of value, ineffectiveness, and long process times in data protection handling in the Swiss education sector. They are based on the concrete experiences of individual EdTech companies and have been generalized in this Whitepaper.

One of the priorities for public authorities and for individual citizens in Switzerland is to establish a flourishing education system, in which all students at all age levels and from all backgrounds can learn and progress in the best possible and most productive way, to become empowered, responsible, competent, and critically thinking citizens. If it is recognized that there are shortcomings - even impediments to competition - in the current rules and regulations, which hinder to reach the above goal, it is essential that those can be tackled and overcome.

In the recent developments of digitization, inadequacies have materialized in a more and more pronounced matter:

- Data Privacy regulations are often applied inconsistently to different tools from different companies, and affect smaller companies and tools in a much more pronounced way than large tech giants
- Data Privacy regulations are not synchronized between the Cantons - tools need to be approved individually in each Canton (Privatim aims to address this)
- Data privacy authorities are understaffed, take long processing time to look at companies, and will not be in a position to consistently process new and coming solutions and keep up with innovations in its current form
- There's a variety of recommendation platforms for schools, which are mostly decentralized, but seem to be understaffed as well as under-resourced (with respect to FTEs and established capabilities and expertise). This leads to the fact that they issue and conclude questionable, wrong, or inadequate recommendations (for example w.r.t. data privacy, pedagogical value, technological edge and user experience for teachers, support services, etc.) - yet those platforms are regarded by teachers as SMA's (Subject Matter Authorities).

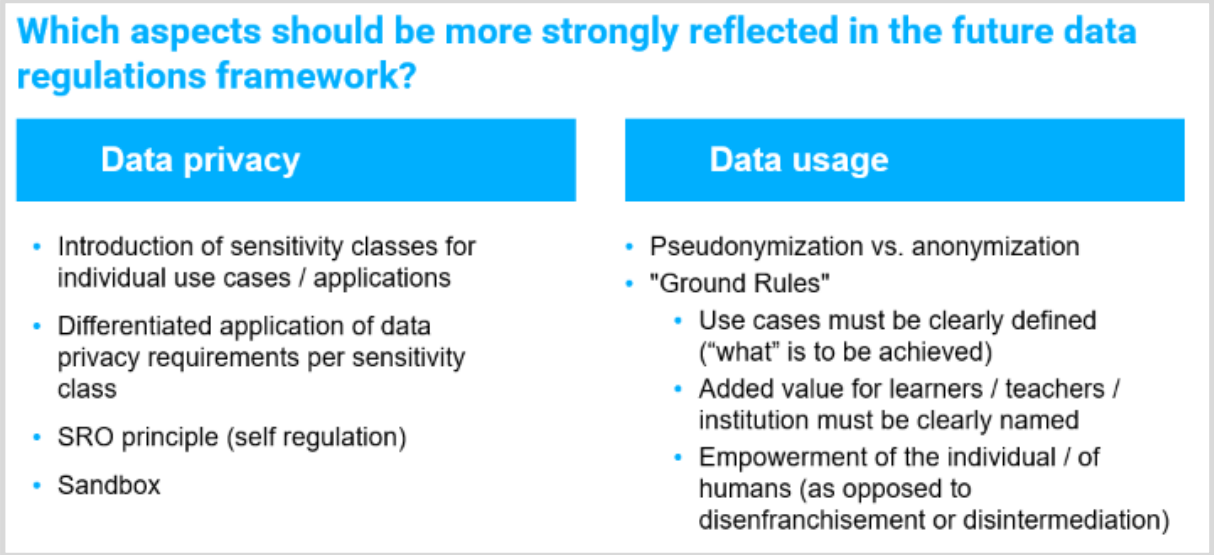
For Swiss EdTech startups there is a lack of certainty which regulations to fulfill. The current "gold standard" seems to be difficult to attain as there are only a handful of companies that were provided with the "gold standard", Privatim's approval and master agreement with Educa. From our perspective, this should not be the case in regards to driving innovation and also it cannot be in the sense of the regulators.

The presented Whitepaper aims at drawing conclusions of what needs to be changed from our perspective always with respect to policies and regulations in the area of data privacy, its enforcement, and its governance. For data privacy to be adequately balanced, there is a framework needed that puts it also into context with its data usage. We believe that also from a data usage perspective the EdTech industry shall adopt certain standards and rules - irrespective of whether they materialize in a hard law, or in standards that are widely adopted and lived through joint commitment.

Introduction

We propose to look at educational data in a more pragmatic way from two perspectives: (1) the perspective of data privacy / protection, and (2) the perspective of data usage. Based on these perspectives, we propose a number of points to consider and to bring together in a new legal framework.

The core elements in those areas, that will subsequently be detailed in this Whitepaper and which we recognize as important building blocks of a new framework, are the following:



Lastly, this paper postulates the consistent enforcement of existing or new regulations, as well as implementation considerations for this new framework.

Elements of a new framework - data privacy perspective

Sensitivity classes

The following sensitivity classes are proposed, into which the individual pedagogical applications are to be divided. Depending on the classification of the sensitivity class, different data protection requirements shall be fulfilled.

Sensitivity class 1 - LOW SENSITIVITY

For use cases where either (1) no personal data is used at all, or (2) only pseudonyms are used, or (3) personal data is used, but in connection with other data that is of little relevance or not meaningful.

Characteristics of sensitivity class 1

- Anonymous use or use under pseudonyms
- No historical trail of the data (historic data points cannot be linked / connected)
- Irrelevant data (no sensitive data of users, e.g. birthdate, real names etc.)

Examples for sensitivity class 1 (list is not exhaustive)

- Learning objectives check under pseudonyms
- Class chat for informal discussions, such as coordination of the next school trip (dates, logistics, packing list, etc.)
- …

Sensitivity class 2 - MEDIUM SENSITIVITY

Use cases that do work with personal data and relate it to other contextual data, however with limited potential of risk and damage.

Characteristics of sensitivity class 2

- Typically authenticated or pseudonymised
- Meaningful/sensitive student data/results but limited in volume and/or history (limited number of students, limited number of data points, aggregation period is limited to 6-12 months) - similar to FINMA's "sandbox" for FinTechs in the financial sector (see link: FINMA Sandbox)

Examples for sensitivity class 2 (not exhaustive)

- Selective monitoring of learning objectives with students, but no holistic use per student over a longer period or over a comprehensive set of subject areas
- Selective and only occasionally used data repositories containing student work, but not structured or only containing fragments / snapshots of the complete student work

Sensitivity class 3 - HIGH SENSITIVITY

Use cases where personal data are processed and linked to other - content-related, process-related and/or contextual - data in such a way that personal profiles are aggregated, which have great significance for the individual and hence bear a higher risk and damage potential.

Characteristics of sensitivity class 3

- Personal data
- Aggregated data / linked data
- Historically available
- Structured and indexable
- Available in large quantities (both per data set and in terms of number of data sets)

Examples for sensitivity class 3 (not exhaustive)

- Grade administration for all students of a school over several years or even decades
- Storage of large numbers of student results over time and different subject areas
- LMS systems which aggregate various data (absences, timetable, student results, communication, etc.)
- ...

Elements of self-regulation & self-declaration

Self-regulation will (1) give more autonomy to the educational institutions/schools in order to use edtech solutions in a controlled manner and according to sound, consistent, practicable, and actually enforceable rules, and (2) allow for a more efficient and effective admission of education technology companies to operate under the required set of rules and standards.

This self-regulation process will entail a self-declaration by respective institutions/schools and education companies. The format and contents of the self-declaration is to be maintained by an institution that has close contact to providers, such as Educa and/or the Swiss EdTech collider.

The following further elements form part of the self-regulation proposal:

- Creation of an admission process for the institution into the SRO (Self-regulation organization)
- Formulation of a declaration of consent for institutions participating in the SRO (Self-regulation organization)
- Establishment of an audit and enforcement process for infringements
- Training of teachers on data protection issues and annual confirmation
- Appointment of a data controller for each training institution (dedicated or shared)
- Establishment of a policy for compliance with essential data protection standards and approval by the school management - "Code of Ethics" (including scope, regulation independence, selection process for tools, operational handling of data management, responsibilities and designation DPO, training, information duties, etc.)
- Awareness-raising for students and parents

Sandbox

Swiss startups and Swiss education companies, yet potentially also other international education software, could take an advantage of a structure where they are allowed to test in teaching and learning settings in a “Sandbox”, similar to the concept of the FINMA sandbox for fintech companies, with lower data protection requirements, as long certain criteria are met.

These criteria could be:

- Limited amount of students (up to X)
- Limited amount of teachers (up to Y per school, total of Z in CH)
- Only used in selective areas (selective subjects)
- Only used for a limited pilot time (e.g., up to 2 years)
- ...

The lower data protection requirements should materialize in the classification of use cases into sensitivity areas.

Foundations and principles for data usage

We believe that independent and irrespective of a more pragmatic legal framework, ethical data usage guidelines for the education sector would be beneficial in general for the education industry and also to speed up the digital transformation in education. The boundaries for data usage use cases are to be measured against such ethical standards:

- **True value-add:** Use cases of data usage need to be always value-adding for and in the interest of
    - The individual (student or teacher) or the education institution (e.g., school), directly, or
    - The larger society (e.g., the collective student body)
- **Data economy:** all use cases of data usage need to be performed in a way that maximizes data economy (“Datensparsamkeit”). Wherever (reasonably) possible, such use cases should employ multiparty computation, pseudonymization, or even anonymization
- **Empowerment of actors:** all use cases of data usage, in particular artificial intelligence, need to be empowering the stakeholders/actors (e.g., they need to make humans smarter and more knowledgeable, e.g., enable them to draw better conclusions, to make more sense of the data, etc.). Under no circumstances shall we push and develop use cases that in the long run lead to a disintermediation and redundancy of human actors

These standards are difficult to formulate in legal terms - which is why first and foremost they shall be formulated as morally and ethically binding standards. Concrete recommendations can be given based on use cases / case examples.

Enforcement

We would like to motivate the following:

1) Legal standards are to be consistently enforced (no loopholes and exemptions for tech giants / “popular” foreign companies). No de jure nor de facto discrimination against Swiss companies. In order to establish this, data privacy relevant parts of the contractual agreements between schools and tech giants need to be made transparent, and it should be possible for other companies to at least use the same standards / agreements
2) Legal standards shall be harmonized across Switzerland (willing “adoption” by the Cantons, nota bene not compromising their authority)

This is not the case today, with examples (with respect to point 1) that most probably have sufficient substance and ground to be contested as infringing competition and stifling innovation, resulting in the legal integrity of the public authorities being at risk.

Implementation considerations

We do not propose to rewrite data privacy law, nor to deviate from the practice of adoption of EU law.

We do propose, however, to make an interpretation of the data privacy law for the education sector, and provide a more pragmatic process and framework, in the form of a:

- Decree ("Verordnung")
- Implementation regulations ("Anwendungsbestimmungen")
- Circular letter ("Rundschreiben")

There are sufficient examples how this can be done, (see for example “online onboarding” in the financial industry).

Next steps

We suggest that both EDK and SBFI take up these proposals and evaluate how these can be implemented, the challenges stated be addressed, and thereby the interests of learners, teachers, education institutions and service providers / startups can best be served in the long term. We’re looking forward to incorporating any feedback to this paper under: whitepaper@edtech-collider.ch.

Supporting Startups as of 1.9.2021
(see also signatures at the end of the document)

- Beecome, represented by John-Edwin Graf
- Classtime AG, represented by Jan Rihak and Valentin Rüst
- Enlightware, represented by Stéphange Magnenat
- Future Instruments AG (Kinaps), represented by Alain Crevoisier
- Getmorebrain, represented by Thomas Gabathuler
- Graasp Association, represented by Denis Gillet
- Hazu, represented by Andy Abgottspon
- Lateral Studio Sàrl, represented by Guillaume Zufferey
- LedSafari, represented by Govinda Upadhyay
- Magma Learning, represented by Maxime Gabella
- MaxBrain, represented by Alex Blattmann and Frank Lyner
- Mira Learning Lab, represented by Tobias Meyer
- Project Herby, represented by Andrin Pelican
- School Rebound SA (Dynamico), represented by Thibault Asselborn
- Smartest Learning, represented by Steve Hinske
- SmartHelio, represented by Govinda Upadhyay
- SpeakUp, represented by Adrian Holzer
- Storm Digital Experiences, represented by Vincent Gschwindemann
- Taskbase, represented by Samuel Portmann
- TestWe, represented by Clément Régnier
- The Experience Accelerator, represented by Sarah Schwab
- Wooclap, represented by Sébastien Lebbe
- Zoe Immersive, represented by Maria Maria Béltran

Appendix

Proposed data protection requirements by sensitivity class

Sensitivity class 1 - low

- Privacy policy and terms of use in place and reviewed
- Applicable law must be defined (but need not be CH or EU)
- Company does not have to be in Switzerland
- Data does not have to be in Switzerland
- Right to delete must be defined and guaranteed
- List of subcontractors available for transparency
- Tracking: Does not require explicit consent, can for example be defined in the general terms and conditions

Sensitivity class 2 - medium

- Applicable law: Switzerland or EU
- Data protection law: Switzerland and EU
- Company does not have to be in Switzerland
- Data does not have to be in Switzerland
- Data must be encrypted
- Support must be clearly defined
- List of subcontractors and DPAs/SCCs available per subcontractor. US subcontractors allowed as long as DPAs and SCCs are available
- Tracking: Only via explicit consent of the users, otherwise tracking cookies may only be set for necessary cookies

Sensitivity class 3 - high

- Applicable law: Switzerland (company must be able to be prosecuted under Swiss law)
- Data protection law: Switzerland AND EU
- Data stored in Switzerland
- Subcontractors may have data abroad, but this must be regulated by DPAs and SCCs (see below).
- High encryption standards
- Support must be clearly defined
- Auditability of the company must be assured and defined
- Data protection authority must be clearly defined
- List of sub-contractors available, conclusion of valid DPAs/SCCs with the sub-contractors (example: assurance of Swiss data protection law). Additional requirements (pseudonymization, encryption) applies to US subcontractors
- Tracking: Only via explicit consent of the users, otherwise tracking cookies may only be set for necessary cookies

Summarizing overview

Criteria	**Class 1 - low**	**Class 2 - medium**	**Class 3 - high**
Privacy policy in place and under review	Yes	Yes	Yes
Terms of use available and checked	Yes	Yes	Yes
Governing law	Defined	CH or EU	CH
Data protection law	Defined	CH and EU	CH and EU
Right to delete	Yes	Yes	Yes
Further rights according to GDPR and CH Data Protection - right of information, correction, limitation of processing, data transferability, opposition	Open	Yes - completely	Yes - completely
Confidentiality	Yes / established	Yes / established	Yes / established
Control rights	Not mandatory	Not mandatory	Yes / established
Subcontractor examination	No	Yes	Yes
Availability	Not guaranteed - as is	Not guaranteed - as is	Guaranteed in accordance with SLAs
Encryption	Strong - at rest and transmission	Strong - at rest and transmission	Strong - at rest and transmission
Data security	Open	Contractually guaranteed	Contractually assured and verifiably defined / documented
Backups	Open	Sensible periodicity / defined	Daily
Advertising	Open	Only with consent	Only with consent
Tracking	Open	Only with consent	Only with consent
… <more to be added if necessary>	...	...	...

Classification of different use cases

Concrete applications for which the various tools and solutions are used can be divided into sensitivity classes. The list below is intended to provide some guidelines for classification. The assigned sensitivity class then specifies which data protection requirements are to be implemented.

The list will hardly ever be complete. If application cases are missing, they can either be added later or, by analogy, be handled in the same way as a similar application case. It is essential that users establish their own awareness and self-responsibility within the framework of the SRO principle. The below are some examples (still need to be finalized):

Use case	**Sensitivity class**
Class chat (not sensitive, anonimised)	1 - low
Regular 1-1 communication	2 - medium
Document storage for teaching materials	1 - low
Collaborative document filing (including personal working documents / papers)	2 - medium
Wikis (not sensitive, anonimised)	1 - low
Class boards	1 - low
Selectively used formative assessments	2 - medium
Aggregated grade report storage	3 - high
Full learning management system with absence management, certificates for sick absences, grade management, communication, student work	3 - high
...	...

General notes

The outlined approach stands in (positive) contrast to the following actual practice

- No or only reluctant action of implementing data privacy policies takes place (data privacy policies being so out-of-touch with reality and are inadequate to cover specific individual needs and cases
- Guidelines are completely ignored, because they cannot be implemented in daily school life or are no longer up-to-date.

Examples: The St. Gallen Secondary School Board maintains a list of platforms, in which essential principles of data protection are handled arbitrarily or deliberately negligently, for example by accepting for certain providers the place of jurisdiction in the USA, or the transfer of data to countries with inadequate data protection guidelines (examples: Socrative, Quizlet, etc.)). Other inconsistent and shockingly unprofessional lists include Zebis, imedias, and others.

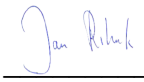
EdTech startup support

The listed EdTech startups below confirm with their signatures, that they support the proposed initiative ‘Data privacy whitepaper - request to decisively address issues in Swiss data privacy regulation in education’.

Date: 08/09/2021

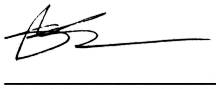
John-Edwin Graf
BEECOME

Date: 03/09/2021



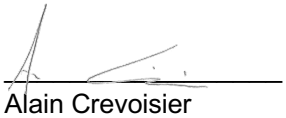
Jan Rihak
CLASSTIME

Date: 06/09/2021



Stéphane Magnenat
ENLIGHTWARE

Date: 16/09/2021



Alain Crevoisier
FUTURE INSTRUMENTS

Date: 03/09/2021

Thomas Gabathuler
GETMOREBRAIN

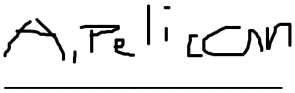
Date: 05/09/2021

Denis Gillet
GRAASP

Date: 06/09/2021

Andy Abgottspon
HAZU

Date: 04/09/2021



Andrin Pelican
HERBY

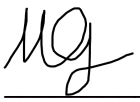
Date: 03/09/2021

Guillaume Zufferey
LATERAL STUDIO

Date: 14/09/2021

Govi Upadhyay
LEDSAFARI

Date: 03/09/2021



Maxime Gabella
MAGMA LEARNING

Date: 09/09/2021

Alex Blattmann
MAXBRAIN

Date: 03/09/2021

Tobias Meyer
MIRA LEARNING LAB

Date: 07/09/2021

Thibault Asselborn
SCHOOL REBOUND

Date: 14/09/2021

Steve Hinske
SMARTEST LEARNING

Date: 14/09/2021

Govi Upadhyay
SMARTHELIO

Date: 06/09/2021

Adrian Holzer
SPEAKUP

Date: 06/09/2021

Vincent Gschwindemann
STORM DIGITAL EXPERIENCES

Date: 14/09/2021

Samuel Portmann
TASKBASE

Date: 14/09/2021

Clément Régnier

Clément Régnier
TESTWE

Date: 03/09/2021

Sarah Schwab
THE EXPERIENCE ACCELERATOR

Date: 16/09/2021

Sébastien Lebbe
WOOCLAP

Date: 10/09/2021

Maria Maria Béltran
ZOE IMMERSIVE

per E-Mail an: jonas.amstutz@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
3003 Bern

Sehr geehrte Damen und Herren

Die Coop-Gruppe (nachfolgend «Coop») bedankt sich für die Gelegenheit, zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellung nehmen zu können. Als Mitglied des Vereins Unternehmens-Datenschutz (VUD) unterstützt Coop die Stellungnahme des VUD. Die vorliegende Stellungnahme geht auf die für Coop wichtigsten Punkte ein.

Grundhaltung Coop: Überregulierung nicht im Sinne des Gesetzgebers

- **Auf zu detaillierte Bestimmungen ist zu verzichten**: Die Vielfalt der Bearbeitungsaktivitäten und Situationen ist so gross, dass Details in aller Regel mehr unbeabsichtigte negative Folgen haben als für Rechtssicherheit zu sorgen. Zudem entwickeln sich digitale Produkte und Dienstleistungen so rasant, dass dem nicht mit Detailregulierungen begegnet werden kann, sondern nur im übergeordneten Rahmen – wie es das revDSG vorsieht.
- **Gesetzliche Grundlage beachten**: Zahlreichen Bestimmungen (Art. 3, 4, 5, 6, 13, 15, 16, 18, 19 Abs. 5, 20 Abs. 5 VE-VDSG) fehlt eine gesetzliche Grundlage oder sie widersprechen gar direkt dem Willen des Gesetzgebers (insbesondere bei neu eingeführten Dokumentationspflichten). Sie sind daher zu streichen. Das gilt insbesondere im Bereich der Datensicherheit (Art.2 VE-VDSG), deren Verletzung zu einer Strafbarkeit führen soll.
- **Übergangsfristen von mindestens 1 Jahr**: Sofern auf Verordnungsstufe tatsächlich neue Verzeichnis- und Dokumentationspflichten eingeführt werden, sind ab Inkrafttreten des revDSG hierfür Übergangsfristen von mindestens einem Jahr vorzusehen.

Coop Genossenschaft
Wirtschaftspolitik
Hauptsitz

Thiersteinerallee 12
Postfach 2550
4002 Basel
Schweiz

Tel. +41 61 336 72 04
Fax +41 61 336 60 40
CHE-116.311.185 MWST

Damian.Misteli@coop.ch
www.coop.ch

Anträge zu einzelnen Artikeln

Artikel 2

Statt «erreichen» ist «anstreben» zu schreiben. Der Katalog der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden. In diesem Fall wäre die Liste auch konform mit Art. 32 DSGVO.

Begründung:
Die Verwendung des Worts «erreichen» impliziert, dass die Schutzziele vollständig erfüllt werden, was weder erforderlich noch möglich ist. Zu treffen sind nur angemessene Massnahmen; eine vollständige Sicherheit ist nicht erforderlich.
Die Regelung zwingt zu einer Dokumentation für jede Datenbearbeitung (u.a. warum bestimmte der aufgeführten Schutzziele nicht relevant sind im konkreten Fall). Das widerspricht dem Willen des Gesetzgebers, der eine solche umfassende Dokumentationspflicht abgelehnt hat.

Artikel 3

Streichen. Es fehlt die gesetzliche Grundlage, die Regelung erreicht das Ziel materiell nicht und zielt an der Sache vorbei.

Begründung:
Die Bestimmung ist problematisch und kann ersatzlos gestrichen werden. Erstens fehlt ihr die gesetzliche Grundlage, zweitens ist das Ergebnis der DSFA kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. In der Regel wird eine DSFA nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenbearbeitung. Dies hat jedoch mit Datensicherheit nichts zu tun. Die Erläuterungen des E-VDSG bestätigen sogar, dass es (auch) um die Gewährleistung der zweckkonformen Bearbeitung geht.

Drittens muss eine solche Bearbeitung kraft Art. 21 revDSG ohnehin dem EDÖB oder Datenschutzberater vorgelegt werden. Eben dies dient bereits dem Ziel, eine solche oder andere Massnahme vorzuschlagen, soweit die Bearbeitung überhaupt umgesetzt werden kann.

Viertens obliegt die Pflicht auch dem Auftragsbearbeiter, der jedoch die DSFA nicht kennen muss und eine solche schon gar nicht auszuführen hat. Massnahmen zur Datensicherheit obliegen zwar auch ihm, aber diese Protokollierung ist in ihrem Kern keine solche. Das erklärt den unlösbaren Widerspruch

Artikel 4

Streichen. Es fehlt die gesetzliche Grundlage. Zudem ist sie unverhältnismässig.

Begründung:
Die Pflicht, für Datenbearbeitungen mit einem hohen Risiko Bearbeitungsreglemente zu erstellen, besteht bereits nach der geltenden Verordnung. Allerdings wurde allgemein erwartet, auch aufgrund der Botschaft des Bundesrats und der parlamentarischen Beratung, dass die Bearbeitungsreglemente angesichts der neu eingeführten Dokumentations- und Informationspflichten (Verzeichnisse von Bearbeitungstätigkeiten, Datenschutz-Folgenabschätzungen, Datenschutzerklärungen) aus der Verordnung gestrichen werden. Das Bearbeitungsreglement dient augenscheinlich nicht der Sicherstellung der Datensicherheit i.e.S., sondern soll primär die Einhaltung der Bearbeitungsgrundsätze und die weiteren Vorgaben des Datenschutzes sicherstellen. Es fehlt der Bestimmung somit eine gesetzliche Grundlage, da Art. 8 revDSG nur Datensicherheit i.e.S. regelt. Der Vorgängernorm fehlt ebenfalls die gesetzliche Grundlage, weshalb sie toter Buchstabe blieb bzw. bleiben musste (ihre Verletzung hat keine Rechtsfolgen). Demgegenüber steht der enorme Aufwand, den die Erstellung und Nachführung eines solchen Bearbeitungsreglements mit sich bringt. Ohnehin werden die wesentlichen Angaben bereits im Rahmen der in solchen Fällen erforderlichen Datenschutz-Folgenabschätzung dokumentiert, der Rest im ohnehin zu erstellenden Inventar. Die Regelung ist somit überflüssig. Auch die DSGVO sieht eine solche Regelung nicht vor (Swiss Finish). Es ist klar, dass besonders heikle Datenbearbeitungen eine betriebsinterne Regelung erfordern können. Dieser Aspekt ist jedoch über Art. 7 Abs. 1 revDSG bereits hinreichend geregelt.

Artikel 13 Abs. 1

Streichen. Die Erwähnung des Auftragsbearbeiters ist zu streichen. Es fehlt die gesetzliche Grundlage.

Begründung:
Art. 13 Abs. 1 E-VDSG verweist auf eine Informationspflicht des Auftragsbearbeiters, was im Erläuterungsbericht auch nochmals ausdrücklich betont wird. Das revDSG sieht aber keine Informationspflicht des Auftragsbearbeiters vor, diese besteht gemäss Art. 19 revDSG (korrekterweise) nur für den Verantwortlichen. Da das Gesetz keine solche Pflicht für den Auftragsbearbeiter vorsieht, kann sie auch nicht über die Verordnung eingeführt werden.

Fazit
Es handelt sich um einen praxisfremden Regulierungsentwurf, welcher oftmals auf einer fehlenden gesetzlichen Grundlage beruht. Die VDSG sollte nur jene Punkte regeln, für die das revDSG ausdrücklich Mindestanforderungen vorsieht, insbesondere bei den Mindestanforderungen der Datensicherheit (Art. 8 Abs. 3 revDSG), bei der Pflicht zur Führung des Bearbeitungsverzeichnisses (Art. 12 revDSG) und bei den Modalitäten des Auskunftsbegehrens (Art. 25ff. revDSG).

Für die Coop-Gruppe sind die zahlreichen im Vorentwurf vorgeschlagenen Dokumentationspflichten nicht realisierbar. Bereits die Erstellung und laufende Aktualisierung des Bearbeitungsverzeichnisses gemäss Art. 12revDSG ist für die Coop-Gruppe enorm aufwändig. Es ist daher unsinnig, weitere Dokumentationspflichten auf Verordnungsweg einzuführen.

Wir danken für die Kenntnisnahme und für die Berücksichtigung unserer Anmerkungen.

Freundliche Grüsse

Coop

Reto Ragettli
Rechtskonsulent, Advokat
Coop Genossenschaft

Damian Misteli
Stv. Leiter Wirtschaftspolitik
Coop Genossenschaft

Creditreform

Per Email:
jonas.amstutz@bj.admin.ch

St. Gallen, den 20. September 2021

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrter Herr Amstutz,
Sehr geehrte Damen und Herren

Wir danken Ihnen für die uns angebotene Gelegenheit, zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) Stellung nehmen zu dürfen. Nachfolgend erhalten Sie fristgerecht unsere Überlegungen zu dieser bedeutenden Umsetzungsnorm im Bereich des Datenschutzes. Dabei nehmen wir vorweg, dass sich unsere Stellungnahme auf den eigentlichen Text des E-VDSG fokussiert und nicht auf alle noch zusätzlichen Verordnungsänderungen (Anhang 2 des Entwurfs). Zudem konzentrieren wir uns, aufgrund unserer Tätigkeit, insbesondere auf den privatrechtlichen Teil der Regelung. Dies bedeutet nicht, dass der öffentlich-rechtliche Teil in allen Punkten unproblematisch erscheint.

1 Allgemeine Vorbemerkung

1.1 Creditreform als Dienstleister im Interesse der Wirtschaft

Seit 1888 widmet sich der Gläubigerverband Creditreform in der Form einer Genossenschaft der Aufgabe, Geschäfte ihrer Genossenschafter sicherer zu machen und sie vor Debitorenausfällen zu bewahren. Es handelt sich um ein modernes, genossenschaftlich strukturiertes Unternehmen und bietet Wirtschaftsauskünfte sowie Inkassodienstleistungen aus einer Hand an. Creditreform verfügt heute über ein Netz von rund 180 Geschäftsstellen in Europa und sieben selbständige Kreisbüros in der Schweiz. Mehr als 165'000 Unternehmen in Europa sind Mitglieder bei Creditreform. Diese beziehen jedes Jahr über 22 Millionen Wirtschafts- und Bonitätsauskünfte.

1.2 Stellung der Genossenschaft im Rahmen des Datenschutzrechts

Durch unsere Tätigkeit bearbeiten wir Personendaten von betroffenen Personen, in der Regel mögliche künftige Vertragspartner unserer Genossenschafter. Dabei ist es wichtig einen Fehler auszuräumen, welcher ab und zu in der Lehre begangen wird. Verschiedentlich werden durch das neue Datenschutzrecht Anforderungen an den Verantwortlichen gestellt, wenn er umfangreich besonders schützenswerte Personendaten bzw. wenn er ein Profiling mit hohem Risiko durchführt. Wirtschaftsauskünfte sind weder von der einen noch von der anderen Tätigkeit betroffen (siehe stellvertretend für andere Beispiele Art. 4 Abs. 1 E-VDSG):

- Zum Einen verarbeitet unsere Genossenschaft keine besonders schützenswerte Personendaten. Im Gegenteil: Sie bezieht eine Vielzahl ihrer Informationen von öffentlich zugänglichen Registern.

- Zum Anderen wird durch die Auskunft über die Bonität eines möglichen Kunden kein Profiling mit hohem Risiko für die Persönlichkeitsrechte der betroffenen Person durchgeführt. Dies aus mehreren Gründen:

  - Erstens ist das hauptsächliche Risiko, welches von der betroffenen Person eingegangen wird, die Zahlungsart für die Lieferung eines Gutes oder die Erbringung einer Dienstleistung. Es geht lediglich darum, die Kreditwürdigkeit einer Person abzuschätzen. Dabei verliert die betroffene Person weder ein Recht noch einen Anspruch, falls die Prüfung ein negatives Bild aufzeigt. Es gibt nämlich weder ein Anrecht noch einen Anspruch auf die Erbringung von Dienstleistungen gegen Kredit. Die betroffene Person kann die Vertragsleistung ohne Weiteres gegen Vorkasse, Barzahlung oder Sicherheiten beziehen, was auch in der Regel die Bezahlungsart bei den meisten Verträgen im täglichen Umgang ist.

  - Im Gegenteil: Die Überprüfung der Kreditwürdigkeit dient sowohl dem Gläubiger als auch dem Schuldner. Dies zeigt bereits das Bundesgesetz über den Konsumkredit vom 23. März 2001 (SR 221.214.1), welches in Art. 22 ausdrücklich die Kreditfähigkeitsprüfung zum Zweck der Vermeidung einer Überschuldung der Konsumentin oder des Konsumenten infolge eines Konsumkreditvertrags vorsieht. Nichts anderes bezweckt die Tätigkeit unserer Genossenschaft. Es ist weder im Sinne des Gläubigers, als auch im Sinne des Schuldners oder der Gesamtwirtschaft, dass die Überschuldung der Konsumenten zu einem Vertrauensverlust führt.

- Die Berechtigung, für den künftigen Gläubiger, seine Leistungen nur bei einer positiven Risikobewertung gegen Kredit zu erbringen, hängt auch sehr stark mit der Ineffizienz der Betreibungs- und Konkursverfahren zusammen. Dafür sei nur auf das Geschäft 19.043 vor dem schweizerischen Parlament und auf unsere Stellungnahme vom 13. September 2021 Verwiesen (siehe Anhang 1). In aller Kürze: Eine statistische Aufarbeitung hat uns gezeigt, dass nur rund 2% der Konkurseröffnungen abgeschlossen werden können. 98% werden aufgrund der Kosten gar nicht beendet. Die beendeten Konkursfälle führen zu einer Konkursdividende der Gläubiger von rund 5% der eingegebenen Forderungen. Der Staat ist gegenwärtig nicht in der Lage, einem Gläubiger ein erfolgsversprechendes Konkursverfahren anzubieten, weshalb es unerlässlich ist, das Gläubigerrisiko entsprechend anders minimieren zu können.

2 Vorbemerkung zum E-VDSG

2.1 Das VDSG als Ausführungsgesetzgebung zum DSG

In rechtsstaatlicher Hinsicht bedarf der Inhalt einer Verordnung einer genügenden Abstützung im Gesetz. Insbesondere muss die Delegationsnorm die vom Bundesrat vorgeschlagene Regelung rechtfertigen. Nicht zulässig ist, in einer Verordnung Regelungen nachzuschieben, welche das Parlament ausdrücklich abgelehnt hat oder Nachbesserungen nachzureichen, an welche im Gesetzgebungsverfahren überhaupt nicht gedacht wurde.

Nicht alle vorgeschlagenen Lösungen im E-VDSG tragen dieser rechtsstaatlichen Anforderung Rechnung. Im Gegenteil: **Der Entwurf enthält Regeln, die entweder ausdrücklich vom Parlament abgelehnt worden sind, die zumindest in systematischer Hinsicht vom Parlament anders gewählt wurden oder an die der Gesetzgeber in keiner Weise gedacht hat. Diese Vorschläge sind allesamt aus dem E-VDSG zu löschen**. Wir verweisen dabei auf die Bemerkungen zu den einzelnen Bestimmungen.

2.2 Das VDSG als Instrument zur Erreichung der Euro-Kompatibilität

Wie beim DSG hat der Bundesrat auch beim E-VDSG in seinen Erläuterungen festgehalten, dass es lediglich um die Angemessenheit des Schweizerischen Datenschutzrechts im Vergleich zur europäischen DSGVO geht. In keiner Art und Weise wurde je von einer Erweiterung der Einschränkungen bei den Datenbearbeitungen bzw. von einer strengeren Regelung gesprochen. Diesem Ziel bleibt also der Bundesrat auch bei der Formulierung des VDSG ausdrücklich verpflichtet. **Alle Bestimmungen, welche also über die Erfordernisse des E-VDSG hinausgehen müssen als zweckfremd und als unzulässig abgelehnt werden. Auch diese sind aus dem E-VDSG zu löschen**.

2.3 Formelle Bemerkung

Zur besseren Lesbarkeit der Verordnung und zum klareren Bezug zum DSG würden wir klare Verweise auf die betroffenen Gesetzesbestimmungen im Titel der jeweiligen Bestimmungen begrüssen. Mit dieser Gesetzgebungstechnik muss sich der Bundesrat klarer und eindeutiger zur Delegationsnorm beziehen, was im vorliegenden Entwurf nur suboptimal gelingt.

3 Zu den einzelnen Bestimmungen

Art. 1 Abs. 1 Bst. d

Als Art. 1 Bst. d werden als Kriterium der Angemessenheit für die Datensicherheit die «Implementierungskosten» genannt. Es wird begrüsst, dass der Aufwand für die Verantwortlichen auch ausdrücklich in die Angemessenheitsüberprüfung aufgenommen wird. Der verwendete Begriff erscheint jedoch problematisch, da er lediglich auf die geldwerten Umsetzungsaufwendungen beschränkt werden könnte (siehe auch S. 16 der Erläuterungen). Für eine solche Einschränkung gibt es keinen Grund. Statt den Begriff «Implementierungskosten» schlagen wir vor den allgemeineren Begriff «**Aufwand für den Verantwortlichen**» zu verwenden. Es gibt keinen Grund, beim Verantwortlichen überhöhte Planungs- oder Projektkosten auszulösen, nur um festzustellen, ob die Implementierung dann ihrerseits verhältnismässig ist.

Art. 1 Abs. 2

Diese Bestimmung verlangt die Überprüfung der technischen und organisatorischen Massnahmen in angemessenen Abständen (gemeint sind hier die zeitlichen Abstände…). Aufgrund des risikobasierten Ansatzes der gesamten Thematik der Datensicherheit erscheint diese Regelung falsch. Zudem führt die Herleitung der Formulierung vom Abs. 1 zur sprachlich merkwürdigen Aussage, dass die dem Risiko angemessenen Massnahmen in angemessenen Abständen zu überprüfen sind. Der Begriff der Angemessenheit riskiert zum Gummibegriff zu verkommen, der jedes Mal verwendet wird, wenn man nichts Präzises auszusagen weiss. Zudem ist fraglich, ob mit der vom Bundesrat aufgestellten Forderung der Überprüfung in angemessenen Abständen die Delegationsnorm von Art. 8 Abs. 3 DSG eingehalten wird. Die Mindestanforderungen an die Datensicherheit rechtfertigen keine Einführung zusätzlicher Kriterien, welche im Gesetz nicht verankert sind. Es ist – wenn überhaupt – in materieller Hinsicht zu fordern, dass ein Zusammenhang zwischen der Überprüfung der Datensicherheit und der Entwicklung des Risikos hergestellt wird. Vorschlag: «**Die Massnahmen sind bei einer relevanten Veränderung des Risikos zu überprüfen.**»

Art. 2, Einleitungssatzes

Die Bestimmung spricht von Zielerreichung. Die jeweiligen Pannen der Swisscom zeigen mit aller Deutlichkeit das auf, was man seit jeher weiss: Die absolute Datensicherheit gibt es nicht. Von den Verantwortlichen zu verlangen, dass die entsprechenden Schutzziele erreicht werden, ist weder korrekt noch realistisch. Der Bereich der Datensicherheit ist ein typischer Bereich, bei welchem keine Ergebnisverantwortung, sondern nur eine Sorgfaltspflicht auferlegt werden darf. Deshalb ist die Bestimmung wie folgt umzuformulieren: «Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele **anstreben**:» Nur so dürfen in der nachfolgenden Aufzählung Begriffe wie «verwehrt», «verunmöglicht», «verhindert», «gewährleistet», usw. überhaupt verwendet werden. Ansonsten müssen in der Aufzählung die Schutzziele jeweils vernünftig relativiert werden, was sicher nicht zur Klarheit der Formulierung beiträgt.

Art. 2, Bst. a bis k:

Art. 2 dürfte eigentlich nur Schutzziele nennen, welche vom Verantwortlichen angestrebt werden können. Gerade die Transportkontrolle kann beispielsweise durch viele externe Faktoren gefährdet werden, für welche der Verantwortliche nicht einstehen kann. Die Aufzählung von Art. 2 Bst. a bis k zeigt in aller Deutlichkeit, was in der Lehre verschiedentlich moniert worden ist: Mangels Effizienz der staatlichen Interventionen, wird die Last der «Privacy by design» vollumfänglich auf den Verantwortlichen abgewälzt, statt dass sie zu datenschutzfreundlichen Technologien durch die Hersteller von Hard- und Software führen würde. Diese Entwicklung zulasten der Nutzer von Informationstechnologien ist im höchsten Masse problematisch, da damit auch der Aufwand für die Datensicherheit dem Betreiber und nicht dem Entwickler von Informationstechnologien auferlegt wird. Die Aufzählung in Art. 2 Bst. a bis k ist in Beachtung dieser Problematik zu überarbeiten und dem Verantwortlichen dürfen nur Schutzziele auferlegt werden, die auch tatsächlich in seiner Verantwortung liegen.

Art. 3

Der Begriff der Protokollierung wird im DSG nirgends verwendet, im Gegenteil z.B. zum neuen Art. 78 Abs. 5 Nachrichtendienstgesetz vom 25. September 2015 bzw. zum neuen Art. 10 Abs. 3 Finanzkontrollgesetz vom 28. Juni 1967. Die nun in der Verordnung vorgesehenen Anforderungen an die Protokollierung übersteigen jedes vernünftige Mass und führen zu einer Bürokratie, welche in keinem Verhältnis zum tatsächlichen Nutzen der Anforderungen steht. Insbesondere die Aufbewahrungsdauer der Protokolle von 2 Jahren (Art. 3 Abs. 4 E-VDSG) ist absolut unangemessen.

Die Protokollierung ist eine qualifizierte Dokumentation der Datenbearbeitung von Personendaten, sagt sie doch ganz klar etwas darüber aus, wer, wann, wie und in welchem Masse Daten der betroffenen Person verarbeitet hat (Art. 3 Abs. 3 E-VDSG). Eine Protokollierung schafft somit ein Spannungsfeld zwischen dem Schutz der betroffenen Person und dem Schutz der verarbeitenden Person. Das Profiling führt zu einer qualifizierten und automatisierten Bearbeitung der Personendaten der datenbearbeitenden Person. Sie bedarf demnach auch einer Rechtsgrundlage im formellen Gesetz, insbesondere dann, wenn die Bearbeitung dieser Personendaten im beruflichen Umfeld zu einem eigentlichen Profiling (Art. 5 Bst. f DSG) und zu einer verpönten Verhaltenskontrolle des Arbeitnehmenden verkommen sollte.

Die nachträgliche Einführung der Protokollierungspflicht im Rahmen der Verordnung erscheint aus Sicht der Wirtschaft nichts anderes als eine unrechtmässige bundesrätliche Nachbesserung eines im Parlament erfolgten Kompromisses, welches zum Verzicht der Protokollierungspflicht geführt hat. Aus Sicht der Wirtschaft genügt die Pflicht der Erstellung die Pflicht zur Erstellung eines Verzeichnisses der Datenbearbeitungen vollumfänglich, um die Rechte und die Interessen der betroffenen Personen zu wahren.

Art. 4

Die Anforderungen von Art. 4 E-VDSG gehen auch viel zu weit. Selbst mit der Einschränkung von Art. 4 Abs. 1 E-VDSG wäre beispielsweise nicht zu verhindern, dass viele Einpersonenunternehmen (Rechtsanwälte, Treuhänder usw.) ein solches Bearbeitungsreglement verfassen müssten. Falls man also diese Pflicht beibehalten muss, ist deren Anwendungsbereich nochmals sorgfältig zu umschreiben und einzugrenzen (schon fast grotesk mutet bei Einpersonenunternehmen nämlich Art. 4 Abs. 3 E-VDSG an).

Allgemein stellt sich die Frage, welchen Mehrwert sich der Bundesrat aus der Führung eines Bearbeitungsreglements neben der Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen erhofft.

Sollte widererwarten am Bearbeitungsreglement festgehalten werden, dann führt die Pflicht, das Bearbeitungsreglement «regelmässig» zu aktualisieren (Art. 4 Abs. 3 E-VDSG) nur dazu, dass eine grosse Mehrheit der Datenbearbeiter dieser Kategorie mit bürokratischen Mitteln in die Illegalität gedrängt werden. Es gibt überhaupt keinen nachvollziehbaren Grund zur «regelmässigen» Überarbeitung des Bearbeitungsreglements. Dieses muss dann überarbeitet werden, wenn es einen Anlass zur Aktualisierung gibt (Veränderung der Bearbeitungsmittel oder Formen).

Art. 5

Obwohl Art. 5 E-VDSG lediglich Bundesorgane betrifft, sei hier lediglich erwähnt, dass eine übertriebene Bürokratie in diesem Bereich zur unnötigen Verschwendung von Ressourcen und Steuergeldern führt, die anderswo wohl effizienter und nützlichere insbesondere für die Empfänger eingesetzt werden können. Wir verzichten auf die erneute Erwähnung dieser Bemerkung in den folgenden Bestimmungen, welche den Ressourceneinsatz der Bundesorgane beeinflussen. Die Bemerkung gilt aber selbstverständlich allgemein.

Art. 6, Abs. 1 und 2

Die Pflicht, für den Verantwortlichen, die vertrags- und gesetzesmässige Bearbeitung durch den Auftragsbearbeiter «sicherzustellen» ist konzeptionell schlicht falsch. Richtig ist, dass der Verantwortliche sich gemäss Art. 9 Abs. 2 DSG vergewissern muss, dass die Datenbearbeitung korrekt erfolgt (korrekt in Art. 6 Abs. 2, 1. Satz E-VDSG). Diese unverhältnismässige, nicht einzuhaltende und nicht vom Gesetzgeber vorgesehene Verschärfung der Pflicht des Verantwortlichen ist im Rahmen der Delegation an den Bundesrat als unrechtmässig zu betrachten. Die Vergewisserung ist ein Streben nach Rechtmässigkeit und eine Kontrollpflicht im Rahmen des Auftrages.

Formulierungsvorschläge für Art. 6 Abs. 1, 2. Satz bzw. Art. 6 Abs. 2, 2. Satz E-VDSG:

Er vergewissert sich, dass die Daten vertrags- und gesetzesgemäss bearbeitet werden.

Andernfalls muss er sich auf dem vertraglichen Weg vergewissern, dass ein gleichwertiger Datenschutz gewährleistet wird.

Art. 6, Abs. 3

Verschiedentlich wird im Gesetz eine «schriftliche» Form verlangt. Es wäre wohl an der Zeit, dass sich der Gesetzgeber ein für allemal dieser Thematik annimmt und entscheidet, ob die «Schriftform» noch zeitgemäss ist, oder ob nicht systematisch die modernere Fassung «*in einer Form, die den Nachweis durch Text ermöglicht*» ersetzen sollte. Natürlich ist der E-VDSG vielleicht nicht gerade die optimale Revision für einen solchen Systementscheid. Es schadet jedoch nichts, dass eine solche Verordnung zukunftskompatibel formuliert wird. Wir verzichten auf die Erwähnung dieser Bemerkung in anderen Bestimmungen, welche die Schriftlichkeit erfordern.

Art. 8

Lediglich im erläuternden Bericht wird klargestellt, an wer sich diese Bestimmung richtet und wen eine Handlungspflicht trifft. Da diese selbstverständlich nicht den privaten Datenbearbeiter betreffen kann, ist dies unmissverständlich im Verordnungstext festzuhalten. Z.B. im Einleitungssatz von Art. 8 Abs. 1 (Änderung in fetter Schrift hervorgehoben): «… *einen angemessenen Schutz gewährleistet,* ***hat der Bundesrat namentlich folgende Kriterien zu berücksichtigen***…».

Art. 9, Abs. 1

Unklar ist, nach welcher Gesetzgebung die Einhaltung der Voraussetzungen gemäss der Aufzählung von Art. 9 Abs. 1 Bst. a – k E-VDSG zu erfüllen sind. Die Kriterien dürfen nicht kumulativ allen möglichen Rechtssystemen unterstellt werden, sonst kann das der Verantwortliche nicht mehr handhaben.

Art. 9 Abs. 2

Auch hier ist die Forderung an den Verantwortlichen überrissen, wenn er «sicherstellen» muss. Auch hier muss er sich «vergewissern».

Art. 10 Abs. 1

Auch hier ist die Forderung an den Verantwortlichen überrissen, wenn er «sicherstellen» muss. Auch hier muss er sich «vergewissern».

Art. 12 Abs. 2 und 3

Es ist unklar, ob die aus Art. 12 Abs. 2 und 3 E-VDSG abgeleiteten Voraussetzungen den Anwendungsbereich von Kodizes und Zertifizierungen nicht unangemessen einschränken. Vielmehr scheint es erforderlich auf die Gesamtwirkung dieser Instrumente zu achten und diese allenfalls vom EDÖB absegnen zu lassen (siehe auch Art. 44 E-VDSG). So könnte z.B. ein Absatz 4 folgendes Ergänzen:

4 Die vorstehenden Absätze 2 und 3 sind nicht anwendbar, wenn der EDÖB den Verhaltenskodex oder die Zertifizierung genehmig hat.

Art. 13 Abs. 1

Gemäss Art. 19 Abs. 1 DSG liegt die Informationspflicht klar beim Verantwortlichen und nicht beim Auftragsbearbeiter. Es kann zwar allenfalls eine vertragliche Delegation der Pflichterfüllung stattfinden, aber grundsätzlich ist es systemwidrig beide gleichzeitig in die Pflicht zu nehmen. Man könnte höchstens das «und» mit einem «***oder***» ersetzen.

Art. 15 und 16

Diese Bestimmungen findet keine Stütze im DSG und sind ersatzlos zu streichen. Die Berichtigung, Löschung, Vernichtung oder Einschränkung der Bearbeitung von Personendaten (Art. 16 E-VDSG) erfolgen zudem im Interesse der betroffenen Person. Diese müssen ja so oder so den Anforderungen des Gesetzes entsprechen. Wieso ausgerechnet in solchen Situationen eine neue Informationspflicht im Interesse der betroffenen Person liegen soll, ist nicht klar. Im Gegenteil: Mit einer solchen Information, sei sie auch so klar, wird die betroffene Person oft verunsichert oder zumindest auf einen Umstand aufmerksam gemacht, der dazu führt, dass Fragen aufgeworfen werden und Aufwand generiert wird, der dem Verantwortlichen nicht entschädigt wird. Das wird von der Wirtschaft in nachvollziehbarer Weise als unnötige und bürokratische Schikane empfunden. Mit einer solchen neuen Pflicht fördert der Bundesrat nicht den Datenschutz, sondern den Datenschmutz. Auf unnötige Informationen ist in den Beziehungen zwischen dem Datenbearbeiter und der betroffenen Person zu verzichten.

Art. 18

Zum Kriterium der Schriftlichkeit, siehe die vorstehende Bemerkung zu Art. 6 Abs. 3 E-VDSG.

Die Aufbewahrungsfrist von **2 Jahren nach Beendigung der Datenbearbeitung** entbehrt einer gesetzlichen Grundlage im DSG und ist als zu lange zu betrachten. Die Aufbewahrung hat höchstens bis zur Beendigung der entsprechenden Datenbearbeitung zu dauern, da danach keine Verletzung der Rechte der betroffenen Person mehr erfolgen kann. Für die Frage, ob jemand durch die Datenbearbeitung ein Schutzrecht der betroffenen Person verletzt hat, ist nicht die

Datenschutz-Folgenabschätzung relevant, sondern die konkrete Datenbearbeitung und die entsprechenden Verzeichnisse und Reglemente des Verantwortlichen.

Art. 19, Erläuterung

In den Erläuterungen des Bundesrates zeigt der Verfasser in den Bemerkungen zu Art. 19, dass er ein merkwürdiges Verständnis der deutschen Sprache hat. «Voraussichtlich» heisst überhaupt nicht, dass die Meldung in jedem «*Zweifelsfall*», in welchem ein «*hohes Risiko nicht ausgeschlossen werden kann*» zu erfolgen hat. Hat die Meldung bei einer «voraussichtlichen Verletzung zu erfolgen, dann ist diese nur vorzunehmen, wenn die Gefahr, dass eine Verletzung der Rechte der Betroffenen Person erfolgt ist, als klar höher einzustufen sind, als die Chancen, dass keine Verletzung erfolgt ist. Der Bundesrat versucht in unrechtmässiger Art und Weise die Einschränkung des Gesetzgebers durch seinen Kommentar umzubiegen.

Art. 19 Abs. 1 Bst. b bis d

Diese Kriterien sind dem Gesetz nicht zu entnehmen. Der Bundesrat hat weder eine Delegation noch eine Ermächtigung erhalten, Art. 24 DSG zu ergänzen. Deshalb sind diese Buchstaben aus der Verordnung zu streichen.

Ar. 19 Abs. 1 Bst. e

Bei der Entdeckung einer Verletzung der Datensicherheit ist es eben gerade nicht immer möglich, die Folgen und die allfälligen Risiken umgehend und abschliessend festzustellen. Deshalb muss beim Bst. e «*soweit möglich*» vorangestellt werden.

Art. 19 Abs. 3

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 Abs. 4 DSG hinausgeht.

Art. 19 Abs. 5

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wiedererwarten an einer Dokumentationspflicht festhalten, schiessen die 3 Jahre weit über das Ziel hinaus. Eine Aufbewahrungsdauer kann höchstens ein Jahr betragen.

Art. 20 Abs. 1 und 2

Zum Kriterium der Schriftlichkeit, siehe die vorstehende Bemerkung zu Art. 6 Abs. 3 E-VDSG.

Art. 20 Abs. 5

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 25 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wiedererwarten an einer Dokumentationspflicht festhalten, schiessen die 3 Jahre weit über das Ziel hinaus. Eine Aufbewahrungsdauer kann höchstens ein Jahr betragen.

Art. 22

Der Fristenlauf kann selbstverständlich nur dann beginnen, wenn das Auskunftsgesuch formell korrekt eingereicht und inhaltlich klar ist. Solange das Gesuch entweder formell oder inhaltlich unklar ist, kann die Frist nicht laufen. Dies muss im Art. 22 E-VDSG in aller Klarheit zum Ausdruck kommen.

Art. 23

Aufgrund der Einschränkungen, die gemäss Abs. 1 für die Kostenbeteiligung vom Bundesrat aufgestellt werden, ist der unveränderte Betrag von CHF 300 geradezu lächerlich. Bei Aufwendungen, die weit über CHF 1'000 gehen können, ist eine Kostenbeteiligung von nur gerade CHF 300.- nicht angemessen. Natürlich hat der Verantwortliche die Kosten zu belegen. Aber es kann nicht sein, dass der Verantwortliche auf einem Kostenberg sitzenbleibt und vom Kostenverursacher nur quasi ein symbolischer Betrag verlangt werden kann. Der Höchstbetrag ist deshalb anzuheben und sollte auf mindestens CHF 1'000 festgelegt werden.

Art. 24

Der Anspruch auf Datenportabilität bei der Datenherausgabe oder -übertragung, darf nicht ein absoluter sein. Dieser Anspruch darf nur bestehen, soweit die Bearbeitung von Personendaten in gängigen Formaten erfolgen kann bzw. erfolgt.

Art. 45 Abs. 1 und 2

Wenn die Kostenbeteiligung nach Art. 23 mit den Gebührengrundsätzen des EDÖB verglichen werden, dann muss von einer krassen Diskrepanz gesprochen werden. Der EDÖB erledigt eine Tätigkeit im Interesse der Gesellschaft und es gibt keinen nachvollziehbaren Grund, weshalb die Person, welche Dienstleistungen von ihm braucht, um sich datenschutzkonform zu verhalten, derart abgeschröpft wird. Weder kann es sein, dass die Gebühren nach Zeitaufwand berechnet werden (die Privatperson hat keinen Einfluss auf die Effizienz der Leistungserbringung durch den EDÖB), noch sind die Stundensätze von CHF 150 bis 350 in irgendeiner Weise angemessen. Diese Gebührenbestimmung stiftet die hilfesuchende Privatperson geradezu an, das Datenschutzrecht zu verletzen, da sie sich die Unterstützung durch den EDÖB nicht leisten kann. Die Gebührenordnung ist vollständig zu überdenken und nach einem vernünftigen Mass anzupassen. Es kann nicht sein, dass der Gesetzgeber einerseits für die Einhaltung des Datenschutzrechts einsteht und andererseits sich durch die Dienstleistungen des EDÖB bereichern will. Hier wird dem service-public-Gedanken in gröbster Art und Weise entgegengewirkt. Es ist erforderlich, Maximalgebühren für Tätigkeiten festzulegen, welche der Einhaltung des Datenschutzrechts dienen (z.B. Art. 59 Abs. 1 Bst. c DSG, Konsultation aufgrund einer Datenschutz-Folgenabschätzung).

Sehr geehrter Herr Amstutz, wir bitten Sie um Kenntnisnahme und um Übernahme der vorstehenden Vorschläge, damit die VDSG in ihrer Rechtssicherheit und in ihrer Rechtmässigkeit entsprechend gestärkt werden kann.

Freundliche Grüsse

Raoul Egeli
Präsident

Prof. Dr. Amédéo Wermelinger
Vizepräsident

curafutura
Die innovativen Krankenversicherer
Les assureurs-maladie innovants
Gli assicuratori-malattia innovativi

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

per E-Mail an: jonas.amstutz@bj.admin.ch

Bern, 14. September 2021

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG): Stellungnahme

Sehr geehrte Damen und Herren

Am 23. Juni 2021 haben Sie das Vernehmlassungsverfahren zur erwähnten Totalrevision der VDSG eröffnet. Gerne nehmen wir dazu wie folgt Stellung.

Allgemeine Bemerkung: Das revidierte Bundesgesetz über den Datenschutz (DSG) sieht keine Übergangsfristen vor. Das neue Recht (Gesetz und Verordnung) müsste also bei dessen Inkrafttreten vollständig implementiert sein. Damit alle Organisationen die neuen gesetzlichen Bestimmungen einführen können, braucht es eine angemessene Umsetzungsfrist. Diese sollte ein Jahr betragen.

Anpassungsvorschläge: Aus dem beiliegenden Dokument entnehmen Sie die Anpassungsvorschläge von curafutura zum Entwurf der VDSG. Die Vorschläge sind priorisiert: «Prio 1» ist wichtig und essenziell. «Prio 2» ist ebenfalls wichtig, jedoch mit geringerer Dringlichkeit.

Für die Kenntnisnahme und Berücksichtigung unserer Stellungnahme danken wir Ihnen bestens.

Freundliche Grüsse
curafutura

Sandra Laubscher
Leiterin Gesundheitspolitik
Stv. Direktorin

Luca Petrini
Projektleiter Gesundheitspolitik

Beilage: Anpassungsvorschläge curafutura

curafutura
Die innovativen Krankenversicherer
Les assureurs-maladie innovants
Gli assicuratori-malattia innovativi

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG): Anpassungsvorschläge curafutura

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
Art. 2 Bst. b	**Prio 2**	b. Zugangskontrolle: Der Zugang zu den Einrichtungen ~~und Anlagen~~, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt.	• Gemäss dem erläuternden Bericht soll mit dem Begriff «Anlagen» insbesondere zum Ausdruck kommen, dass auch der Zugang zu mobilen Bearbeitungsanlagen zu unterbinden ist. Der Begriff ist sehr weit gefasst und umfasst von fest angelegten Serveranlagen über den Computer bis hin zu Mobiltelefonen oder Tablets jegliche Geräte zur Bearbeitung von Personendaten. Eine Zugangskontrolle zu Mobiltelefonen oder Tablets ist schlicht unrealistisch. Gerade in der Pandemiezeit mussten alle Mitarbeitenden zu Hause arbeiten, wobei nicht jeder über eine eigene Wohnung verfügt, wo der Zugang zu tragbaren Mobilgeräten kontrolliert erfolgt. Wichtig ist lediglich, dass sich kein Unberechtigter Zugriff verschaffen kann. Hier muss die Zugriffskontrolle ausreichen.
Art. 2 Bst. c, d und g	**Prio 2**	c. Datenträgerkontrolle: Das ~~Lesen, Kopieren, Verändern, Verschieben~~ Bearbeiten von Personendaten auf dem Datenträger oder das Entfernen von Datenträgern wird unbefugten Personen verunmöglicht. d. Speicherkontrolle: Unbefugte ~~Eingabe in den~~ Bearbeiten der Personendaten im Datenspeicher ~~sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten~~ wird verhindert.	• Die zahlreichen Aufzählungen (Veränderung, Löschung usw.) mit Bearbeiten ersetzen. Mit dem Begriff des Bearbeitens werden sämtliche Datenbearbeitungen erfasst, was der Terminologie des DSG entspricht. • Der Unterschied zwischen Datenträger (Bst. c) und Datenspeicher (Bst. d) ist ebenso unklar, wie, ob sich die Verben auf den Datenträger beziehen oder rein auf die Daten, welche darauf enthalten sind. Es sollte zwischen Bearbeitung von Daten auf dem Datenträger und dem Datenträger als

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
		g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person ~~eingegeben oder verändert~~ bearbeitet wurden.	Physischem differenziert werden. Es sollten einheitliche Begriffe verwendet werden.
Art. 3 Abs. 1	**Prio 2**	1 Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, ~~Lesen,~~ Bekanntgeben, Löschen oder Vernichten.	• Auf die Protokollierung des «Lesen», was kaum umsetzbar sein wird, ist zu verzichten.
Art. 3 Abs. 2	**Prio 1**	**Streichen**	• Eine pauschale Protokollierungspflicht der Bundesorgane für alle automatisierten Bearbeitungen von Personendaten lehnen wir ab. Es fehlt hierfür eine Rechtfertigung bzw. im erläuternden Bericht (Seite 20) wird auf Art. 25 der EU-Richtlinie 2016/680 verwiesen. Sollte wegen dieser EU-Bestimmung aus Äquivalenzgründen eine einschlägige Regelung auf Verordnungsstufe notwendig sein, ist diese auf den Strafrechtsbereich zu limitieren. • Für den Nicht-Strafrechtsbereich, z.B. den Sozialversicherungsbereich, sollte Absatz 1 zur Anwendung kommen.
Art. 3 Abs. 4	**Prio 2**	4 Die Protokolle sind während einem ~~zwei~~ Jahr~~en~~ ~~getrennt vom System, in welchem die Personendaten bearbeitet werden,~~ aufzubewahren und vor nachträglicher Veränderung zu schützen. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit	• Es ist die geltende Aufbewahrungsfrist von einem Jahr beizubehalten (siehe Art. 10 Abs. 2 VDSG). • Die Begründung, wonach sich Cyber-Angreifer in der Regel länger in einem System aufhalten, ohne erkennbaren Schaden anzurichten, ist nicht stichhaltig für eine Erhöhung der

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
		und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.	Aufbewahrungsfrist. Wenn ein Angreifer nur beobachtet, ohne Veränderungen vorzunehmen, dann sieht man das nicht und schafft mit einer Verlängerung der Aufbewahrungsfrist nur einen Mehraufwand. Die Herausforderung dabei ist, die gesammelten Protokolldaten sinnvoll auszuwerten. Eine Auswertungslösung, wie beispielsweise Splunk, erfordert bei einer grösseren Datenmenge eine Erweiterung der Lizenz, was mit hohen zusätzlichen Kosten verbunden ist, ohne dass dadurch ein höheres Schutzniveau erreicht wird. • Nicht zielführend ist auch das Erfordernis einer getrennten Aufbewahrung, da sich ein Angreifer auch in getrennten Systemen gleichzeitig bewegen kann. Zielführender wäre eine Vorgabe, wonach die Protokolle vor nachträglicher Veränderung zu schützen sind. Im Übrigen kann mit der Protokollierung alleine wohl kaum ein Cyberangriff aufgedeckt werden. Es braucht dafür eine Korrelation über verschiedene Systeme hinweg, angefangen beim Client, mit dem die Benutzer arbeiten, über Server und Datenbanken, auf die sie zugreifen, bis hin zu Netzwerkaktivitäten, welche dann in der Korrelation als Anomalie entdeckt werden können.
Art. 4	**Prio 1**	**Streichen**	• Es fehlt eine ausreichende gesetzliche Grundlage. Wichtiges, wie Pflichten gehören ins Gesetz (Art. 164 Bundesverfassung). Eine solche zusätzliche Pflicht hätte im Gesetz selbst geregelt werden müssen. Die Dokumentationspflicht wurde im Rahmen des Gesetzgebungsprozesses auf das

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
			Führen des Bearbeitungsverzeichnisses eingeschränkt, so dass diese Bestimmung dem widerspricht. • Diese Bestimmung ist zudem redundant zum Verzeichnis der Bearbeitungstätigkeiten (VBT) gem. Art. 12 des revidierten DSG. Das Verhältnis zu den VBT ist unklar und die erforderlichen Informationen sind in den VBT enthalten. Dies beutete einen beträchtlichen Dokumentationsaufwand, da ein grosser Teil der Angaben doppelt (im Bearbeitungsreglement und im Bearbeitungsverzeichnis) geführt werden müsste. • Zudem wird der Mehrwert des Bearbeitungsreglements im Sinne der Transparenz stark angezweifelt. Zumal mit dem Verzeichnis der Bearbeitungstätigkeiten (VBT) ein Instrument geschaffen wurde, welches das Reglement nach geltendem Recht ersetzt und im Falle von Bundesorgangen ebenfalls dem EDÖB gemeldet werden muss. Es ist unverständlich, warum das Reglement nun über die Verordnung durch die Hintertüre eingeführt werden soll, vor allem, wenn gewisse Angaben sogar aus dem Verzeichnis «kopiert» werden sollen, was jedoch kaum so einfach umsetzbar sein wird. • Die technischen und organisatorischen Massnahmen sind Pflichten des Verantwortlichen, wie auch die Protokollierung der Zugriffsberechtigungen und der Zugriffe, womit sich eine Publikation erübrigt. Im Gegenteil wird sogar ein Risiko für die Verantwortlichen geschaffen, wenn betroffene Personen

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
			versuchen, über das Auskunftsbegehren Einsicht in das Reglement zu erhalten. • Weitere Angaben im Reglement müssen über die Informationspflichten ohnehin erfüllt werden. Mit einem Bearbeitungsreglement wird nur ein zusätzlicher administrativer Aufwand geschaffen, der keinen zusätzlichen Nutzen für die betroffenen Personen bringt. Aus diesen Gründen ist auf ein zusätzliches Bearbeitungsreglement zu verzichten.
Art. 5	**Prio 1**	**Streichen**	• Siehe Begründung unter Artikel 4. • Konsequenterweise sollte bei einer Streichung von Art. 5 auch Art. 84b KVG bei einer künftigen Revision des KVG entsprechend angepasst werden.
Art. 6 Abs. 1	**Prio 1**	1 Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er ~~muss sicherstellen~~ sorgt dafür, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.	• Der Verantwortliche kann nicht sicherstellen, sondern bloss für die vertrags- und gesetzesgemässe Bearbeitung sorgen (lassen). • Unklar ist, warum «auftragsgemäss» gemäss geltendem Art. 22 VDSG durch «vertrags- oder gesetzesgemäss» ersetzt werden soll.
Art. 6 Abs. 2	**-**	-	• Wir gehen davon aus, dass in Bezug auf Art. 6 Abs. 2 die Länderliste im Anhang 1 der revidierten VDSG Anwendung findet.
Art. 6 Abs. 3	**Prio 1**	3 Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich oder in einer anderen Form, die den Nachweis durch Text ermöglicht,	• Im Zuge der fortschreitenden Digitalisierung ist neben der Schriftform (Erfordernis der eigenhändigen Unterschrift gemäss OR) alternativ auch Textform möglich (siehe z. B. revidiertes VVG, das per 1. Januar 2022 in Kraft tritt und

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
		genehmigt hat oder nicht innert angemessener Frist widerspricht.	neu grossmehrheitlich die Textform alternativ neben der Schriftform vorsieht). • Zudem sollte anstelle einer Genehmigung alternativ auch ein Widerspruchsvorbehalt möglich sein.
Art. 7	**Prio 2**	**Streichen**	• Überflüssig, da der Berater bei der Anwendung des Datenschutzrechts gemäss revidiertem DSG mitwirkt. • Bundesorgane, wie bspw. Krankenversicherungen haben unzählige Verträge, welche eine Auftragsdatenbearbeitung beinhalten. Hier ist ein risikobasierter Ansatz zu wählen. Der Datenschutzberater/die Datenschutzberaterin kennt die besonders risikobehafteten Bearbeitungen durch das Verzeichnis der Bearbeitungstätigkeiten. Eine zusätzliche Informationspflicht – zumal in dieser Absolutheit – ist überflüssig und schafft keinen Mehrwert für die betroffenen Personen.
Art. 9 Abs. 1 Bst. j	**Prio 2**	**Streichen**	• Die Datenschutzklauseln sollen die Pflicht des Empfängers enthalten, die betroffenen Personen zu informieren. Es ist nicht Aufgabe des Auftragsberarbeiters, die betroffenen Personen zu informieren, dies ist Aufgabe des Verantwortlichen.
Art. 13 Abs. 1	**Prio 1**	1 Der Verantwortliche ~~und der Auftragsbearbeiter~~ teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit, wobei ein Verweis auf eine Datenschutzerklärung auf der Website oder auf allgemeine Geschäftsbedingungen ausreichend ist.	• Eine Informationspflicht des Auftragsbearbeiters ist nicht praktikabel und unnötig. Der Auftragsbearbeiter erledigt seine Aufgaben nach Weisung und ausschliesslich nach dem vom Verantwortlichen vorgegebenen Zweck. Es kann nicht sein, dass hier eine Informationspflicht des Auftragsbearbeiters eingeführt wird. Das wäre auch keinesfalls durch eine Gesetzesdelegation gedeckt.

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
			• Im Interesse der Rechtssicherheit ist zudem klarzustellen, wie der Informationspflicht nachgekommen werden kann. • Der Verweis auf eine Website oder auf allgemeine Geschäftsbedingungen muss in der heutigen Zeit genügen.
Art. 13 Abs. 2	**Prio 2**	**Streichen**	• In der vorgesehenen Formulierung nicht praktikabel. • Es ist unklar, was maschinenlesbar bedeutet.
Art. 14	**Prio 2**	Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin, sofern dies aus den Umständen nicht ersichtlich ist.	• Die Freiwilligkeit kann auch aus den Umständen ersichtlich sein, so dass ein Hinweis nicht notwendig ist.
Art. 15	**Prio 1**	**Streichen**	• Es fehlt eine gesetzliche Grundlage. • Diese Pflicht scheint nicht umsetzbar/nicht praktikabel. • Letztlich ist es Sache der Verantwortlichen, die Einhaltung der Datenschutzgrundsätze sicherzustellen. Bei gesetzlich vorgesehenen Datenbearbeitungen ist die Information ohnehin unnötig. • Bezüglich einer Pflicht des Auftragsbearbeiters kann auf die obgenannten Ausführungen verwiesen werden.
Art. 16	**Prio 1**	**Streichen**	• Es fehlt eine gesetzliche Grundlage. • Diese Pflicht wurde im Rahmen des Vernehmlassungsverfahrens gestrichen (war in Art. 19 Bst. b Vorentwurf DSG). Es gibt keine Delegationsnorm hierzu, müsste auf Gesetzesstufe geregelt werden.
Art. 18	**Prio 2**	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in einer anderen Form, die den Nachweis durch	• Siehe auch Ausführungen unter Art. 6 Abs. 3.

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
		Text ermöglicht, festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.	• Schriftlichkeit ist weder erforderlich noch zeitgemäss (Digitalisierung). Neben der Schriftform (Erfordernis eigenhändiger Unterschrift gemäss OR) muss alternativ auch Textform möglich sein (siehe z.B. revidiertes VVG, das per 1. Januar 2022 in Kraft tritt und neu grossmehrheitlich die Textform alternativ neben der Schriftform vorsieht).
Art. 18 Abs. 2 zusätzlich	**Prio 2**	*2 Bundesorgane müssen bei gesetzlich vorgesehener Datenbearbeitung keine Datenschutz-Folgenabschätzung vornehmen.*	• Bei gesetzlich vorgesehenen Datenbearbeitungen ist es nicht opportun, noch eine Datenschutz-Folgenabschätzung von den Bundesorganen zu fordern. • Es ist auch auf den erläuternden Bericht zu verweisen, wonach vorgesehen werden soll, dass die Bundesorgane die Datenschutz-Folgenabschätzung zusammen mit den Erlassentwürfen dem Antrag an den Bundesrat beifügen müssen und sie die Resultate der Datenschutz-Folgenabschätzung in der Botschaft des Bundesrats festhalten müssen. Immerhin kann somit in der Verordnung festgehalten werden, dass bei gesetzlich vorgesehenen Datenbearbeitungen keine Datenschutz-Folgenabschätzung mehr notwendig ist.
Art. 19 Abs. 5	**Prio 2**	5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens ~~drei~~ ein Jahre aufzubewahren.	• In der ganzen Verordnung finden sich unterschiedliche Aufbewahrungsfristen. Das ist umständlich, prozessual mühsam und auch wenig zweckmässig. Eine einheitliche Aufbewahrungsfrist von einem Jahr erscheint angemessen.
Art. 20 Abs. 3	**Prio 2**	3 Die Auskunft muss ~~für die betroffene Person~~ in einer Landessprache oder Englisch und verständlich verfasst sein.	• Sofern sich die Verständlichkeit auf die Sprache bezieht, so ist diese Anforderung auf die Landessprachen und Englisch

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
			zu begrenzen. Ansonsten müsste in jeder Sprache Auskunft gegeben werden.
Art. 20 Abs. 5	**Prio 2**	5 Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens ~~drei~~ ein Jahr~~e~~ lang aufzubewahren.	• Vgl. Art. 19. Insbesondere ist nicht einzusehen, warum die Dokumentation der Verweigerung, Einschränkung oder des Aufschubs einer Auskunft länger aufbewahrt werden muss, als die Protokolle gemäss Art. 3.
Art. 23 Abs. 2	**Prio 2**	2 Die Beteiligung beträgt maximal 300 Franken.	• Die Kostenbeteiligung sollte den Umständen Rechnung tragen. Eine Fixierung auf max. 300 Franken ist nicht sachgerecht. Die max. Beteiligung ist angemessen zu erhöhen.
Art. 25 Abs. 1 Bst. a	**Prio 2**	a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden.	• Der Datenschutzberater muss nicht jede Bearbeitung prüfen, es gilt der risikobasierte Ansatz.
Art. 31	**Prio 1**	**Streichen**	• Es fehlt eine ausreichende gesetzliche Grundlage. Diese Informations- bzw. Meldepflichten sollten, wenn schon im Gesetz geregelt werden. • Ausserdem unklare Formulierungen, insbesondere die Begriffe «rechtzeitig» und «nach Abschluss des Projekts».
Art. 32	**Prio 1**	**Streichen**	• Siehe auch Ausführungen unter Art. 31. • Von einer Meldung an den EDÖB ist abzusehen. Ein Sinn für die Meldepflicht an den EDÖB ist nicht ersichtlich. • Bundesorgane müssen nach Art. 12 Abs. 4 des revidierten DSG das Verzeichnis ihrer Bearbeitungstätigkeiten dem EDÖB melden. Eine zusätzliche Pflicht zur Meldung jeder geplanten automatisierten Bearbeitungstätigkeit bringt keinen

E-VDSG	Priorität	Anpassungsvorschlag	Begründung
			Mehrwert für die betroffenen Personen, führt zu einem unnötigen administrativen Aufwand für die Bundesorgane und zu einer Aufblähung des staatlichen Apparates (siehe auch begrenzte personelle Ressourcen des EDÖB, der alle diese Meldungen sichten müsste).
Art. 43	**-**	-	• Hinweis: vgl. Art. 32. Im Falle einer Streichung von Art. 32 ist Art. 43 entsprechend anzupassen.
Art. 47	**-**	-	• Hinweis: vgl. Art. 32. Im Falle einer Streichung von Art. 32 ist auch Art. 47 zu streichen.

Bern, 12. Oktober 2021

Ausführungsrecht zum Datenschutzgesetz (revidierte Verordnung über den Datenschutz)

Vernehmlassungsantwort von CURAVIVA Schweiz

Sehr geehrte Damen und Herren

Im Rahmen der vom Bundesrat eröffneten Vernehmlassung über die Revision der Verordnung über den Datenschutz reicht der nationale Branchenverband CURAVIVA Schweiz reicht die vorliegende Stellungnahme ein.

Gemeinsam mit den Mitgliederinstitutionen ist CURAVIVA Schweiz für die Menschen da, die auf individuelle Begleitung, Pflege und Betreuung angewiesen sind. Für Kinder und Jugendliche, für Menschen mit Behinderung, für Menschen im Alter. Als nationaler Branchenverband vertritt CURAVIVA Schweiz landesweit über 2'700 Institutionen. Die Mitgliederinstitutionen bieten rund 120'000 Menschen ein Zuhause und beschäftigen mehr als 130'000 Mitarbeitende.

I. Ausgangslage

Die DSG-Totalrevision umfasst zum einen eine Totalrevision des DSG (E-DSG), zum andern eine Teilrevision weiterer Bundesgesetze. Das Parlament hat die Vorlage des Bundesrates in zwei Etappen aufgeteilt. In der ersten Etappe wurde nur eine EU-Richtlinie zum Datenschutz in Strafsachen (SDSG) umgesetzt und am 1.3.2019 in Kraft gesetzt. In der zweiten Etappe hat das Parlament das neue Datenschutzgesetz (nDSG) am 25.9.2020 verabschiedet. Die vorliegende Vernehmlassung über das Umsetzungsrecht des revidierten DSG (Vorentwurf der revidierten Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)) wurde am 23.6.3021 eröffnet. Sie dauert bis am 14.10.2021.

II. Vernehmlassungsunterlagen

- Vernehmlassungsvorlage
- Erläuternder Bericht
- Begleitschreiben an die Verbände usw.

III. Grundzüge der vorliegenden Vernhemlassungsantwort

Im Rahmen des vorliegenden Verfahrens haben die Verbände CURAVIVA Schweiz, INSOS Schweiz, senesuisse und Spitex Schweiz eng zusammengearbeitet, so dass ihre Vernhemlassungsantworten inhaltlich übereinstimmende Standpunkte vertreten.

Da es sich im Rahmen der vorliegenden Vernehmlassung nur noch um die Gestaltung des Umsetzungsrechts einer bereits erfolgten Gesetzesrevision handelt, ist der Ermessenspielraum für Anpassungen der neuen Gesetzgebung sehr begrenzt.

Die vorliegende Vernehmlassungsantwort fokussiert auf die für die Institutionen und Strukturen für Menschen mit Unterstützungsbedarf relevanten Punkte der vom Bundesrat vorgeschlagene VDSG-Revision.

In der vorliegende Vernehmlassungsantwort wird in erster Linie darauf geachtet, dass die vom Bundesrat vorgeschlagenen Umsetzungsmodalitäten des revidierten Datenschutzgesetzes möglichst schlank, praxisnah und anwendungsfreundlich für die Betriebe bleiben. Das ist nicht selbstverständlich im Rahmen eines Gesetzgebungsprozesses, der nicht besonders darauf ausgerichtet ist: Dieser strebt offensichtlich vor allem eine sehr genaue und umfangreiche Einhaltung des Datenschutzes an.

Des Weiteren beantragt die vorliegende Vernehmlassungsantwort eine möglichst konkrete, zugängliche und auch finanziell günstige Unterstützung der Betriebe durch die zuständigen staatlichen Stellen – vor allem durch den Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Die in der Stellungnahme vertretenen Standpunkte berücksichtigen gleichwohl die Wichtigkeit eines zielführenden Datenschutzes: Allgemein wird davon ausgegangen, dass die Betriebe oftmals heikle Daten bearbeiten, deren Bekanntgabe ein hohes Risiko für die betroffenen Personen von Unterstützungsleistungen aufweisen können; deswegen soll an einem strikten Datenschutz nicht gerüttelt werden.

Auch wird in der vorliegenden Vernehmlassungsantwort beantragt, dass grob umrissene Begriffe und Abgrenzungen präziser umschrieben werden – dies im Sinne einer möglichst klaren Umsetzungshilfe für die betroffenen Betriebe.

IV. Relevante Bestimmungen der E-VDSG für die ambulanten und stationären Betriebe für Personen mit Unterstützungsbedarf

E-VDSG	Kommentar	Beantragte Neuformulierung
Art. 1 Abs. 1	Die vorgeschlagene Umschreibung ist im Grundsatz zu begrüssen. Sie ergänzt und konkretisiert sinnvollerweise Artikel 8 Absatz 1 nDSG. Zu begrüssen ist, dass sie möglichst schlank und angesichts der stetigen technischen Entwicklungen flexibel, praxisnah und anwendungsfreundlich gehalten worden ist. Weil sie sehr allgemein formuliert ist, braucht es aber entsprechenden Deutungs- und Umsetzungshilfen für die Praxis.	- Es müssen seitens EDÖB möglichst bald Dokumente geschaffen werden, welche den Betrieben die Praxisumsetzung vereinfachen.

Art. 1 Abs. 2	Die Abstände zwischen den vorzunehmen Überprüfungen sollten präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Was genau „angemessene Abstände“ sind, hängt selbstverständlich von den Besonderheiten des konkreten Anwendungsfalls ab (S. 17 im erläuternden Bericht: «[…] bei der Bestimmung der Massnahmen selbstredend die Umstände des Einzelfalls massgeblich [bleiben]»). Während die Datenbearbeiter inhaltlich grossen Freiraum für die Bestimmung ihrer konkreten Massnahmen brauchen, sollte zeitlich zumindest eine konkrete Anforderung gelten, um die Sicherheit zu gewährleisten. Als sinnvoll erscheint uns eine mindestens jährliche Überprüfung.	[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen, jedoch mindestens einmal pro Jahr zu überprüfen.
Art. 2	Diese präzise Auflistung der Schutzziele macht Sinn: Sie stellt eine praxisorientierte ‚Gedächtnisstütze‘ für die Verantwortlichen und die Auftragsbearbeiter dar, was im Rahmen ihrer Konkretisierung zu berücksichtigen ist. Wichtig ist eine gute Anwendbarkeit in der Praxis (Seite 17 des Berichts: „In Anwendung der Verhältnismässigkeit sind ausgehend [… von dieser Auflistung der Schutzziele] die organisatorischen und technischen Massnahmen des Einzelfalls zu bestimmen.“). Gleichzeitig zeigt diese Auflistung die Komplexität der Anforderungen an eine gesetzkonforme Datenbearbeitung und -sicherheit auf - mit dem damit verbundenen Aufwand. Aus diesem Grund ist eine möglichst konkrete und für Schweizer Betriebe auch unentgeltliche Unterstützung der Datenschutzverantwortlichen durch die zuständigen Behörden (insbesondere das EDÖB), vorzusehen. So können die Umsetzungskosten für Wirtschaft und Gesellschaft minimiert und angemessene Datensicherheit auf allen Ebenen geschaffen werden.	- Für eine optimale und kostengünstige Umsetzung ist darauf zu achten, dass Schweizer Unternehmen einen guten und kostengünstigen Zugang zum EDÖB erhalten (vgl. auch Art. 45 Abs. 2).
Art. 3	Welche „Massnahmen“ im vorliegenden Rahmen berücksichtigt werden sollen und ob ein Risiko als hoch oder begrenzt eingeschätzt werden soll, dürfte in der Praxis oftmals schwierig zu beurteilen sein, denn Artikel 8 nDSG führt auch keine präziseren Anhaltspunkte über die Art der infrage stehenden Massnahmen. Dies entspricht zwar einer flexiblen, bedarfsorientierten und dem neusten technischen Stand angepassten Umsetzung des Datenschutzes, macht aber dessen Realisierung in der Praxis schwierig. In diesem Sinne ist die Präzisierung der Inhalte der Protokollierung (gemäss Abs. 3) an sich konsequent und kongruent. Sie weist aber einen hohen Detaillierungsgrad auf, der einen entsprechend hohen Umsetzungsaufwand, eine Unübersichtlichkeit und mögliche Verwechslungsrisiken mit sich bringt.	In Art. 3 Abs. 1 müssen Alternativen zur im Entwurf vorgesehenen (komplexen) Protokollierung – ausdrücklich vorgesehen und auch aufgezählt werden, namentlich Zugriffskontrollen, die physische/räumliche Sicherung der Daten, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.

	Es ist festzustellen, dass gerade bei der *automatisierten* Bearbeitung von Personendaten die Anforderung einer detaillierten Protokollierung einen beträchtlichen Teil der Vorteile der Automatisierung beraubt: Der zeitliche und administrative Aufwand wird dadurch erheblich vergrössert. Trotzdem erscheint uns eine Protokollierung richtig, sofern keine anderen Massnahmen das gleiche Ziel mit weniger Aufwand erreichen können. *Antrag:* Alternativen zur Protokollierung als Massnahmen zum Datenschutz sollen im E-VDSG ausdrücklich vorgesehen und auch aufgezählt werden – wie etwa die physische/räumliche Sicherung der Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.	
Art. 4 Abs. 2	Weil in sehr vielen Fällen eine automatisierte Bearbeitung von besonders schützenswerten Personendaten erfolgt, sind die von dieser Bestimmung gestellten Anforderungen als zu aufwendig und vielfach unnötig zu qualifizieren. Sie bringen für die betroffenen Datenbearbeiter unangemessen hohe Kosten mit sich. Deswegen ist diese Auflistung zu kürzen: Die Buchstaben d, e und j sollen ersatzlos gestrichen werden, weil sie unnötige zusätzliche Anforderungen und Präzisierungen darstellen, die den administrativen Aufwand für die Betriebe verschärfen, ohne dass daraus ein entsprechender Nutzen entsteht. Buchstabe i soll gekürzt werden: Er weist einen Detaillierungsrad mit entsprechenden Umsetzungskosten auf, der in keinem vernünftigen Verhältnis zu seinem Nutzen steht. Hingegen werden Buchstaben a, b, c, f und g ausdrücklich begrüsst, da sie zentrale Massnahmen zur Gewährleistung der Datensicherheit darstellen. Ihre Einhaltung genügt, um dem Datenschutz gerecht zu werden. Auch Buchstabe h wird begrüsst, weil eine stets angestrebte Datenminimierung das beste Mittel darstellt, um sowohl den Schutz der Privatsphäre als auch die Verminderung des mit jeglichem Datenbearbeitung verbundenen administrativen Aufwands zu erreichen.	[2] Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. ~~zur internen Organisation~~; e. ~~zur Herkunft der Personendaten und zur Art ihrer Beschaffung~~; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den ~~Datenbearbeitungsverfahren, insbesondere den~~ Verfahren bei der Speicherung, ~~Berichtigung, Bekanntgabe, Aufbewahrung, Archivie-~~

		~~rung,~~ Pseudonymisierung,~~-~~Anonymisierung und Löschung oder Vernichtung; j. ~~zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.~~
Art. 4 Abs. 3	Wie gemäss obigem Antrag zu Art. 1 Abs. 2 sollten auch hier die zeitlichen Abstände zwischen den vorzunehmen Aktualisierungen präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Deswegen wird hier beantragt, dass die Aktualisierungen mindestens einmal jährlich stattfinden: Dieser Zeitabstand stellt eine präzise, zugleich realistische und daher auch anwendungsfreundlich Leitplanke dar.	[3] Die private Person muss das Reglement ~~regelmässig~~ in angemessenen Abständen, jedoch mindestens einmal pro Jahr, aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.
Art. 6 Abs. 2	Die in dieser Bestimmung gestellten Anforderungen an die Verantwortlichen betreffend dem DSG nicht unterstellten Datenbearbeiter sind offensichtlich zu hoch. Von einem Verantwortlichen kann vernünftigerweise nicht verlangt werden, dass er Kenntnis der vielen potenziell relevanten Gesetzesbestimmungen und der möglichen Abhilfe-Lösungen hat. Wenn schon ist es die Pflicht von Gesetzgeber und Verwaltung, den Datenschutz so auszugestalten, dass dieser – wo nötig und sinnvoll – überall für alle Betroffenen gleichermassen gilt. Diese Pflicht den einzelnen Verantwortlichen aufzubürden, wie der Bundesrat es vorschlägt, führt zu enormer Unsicherheit und Aufwand. Deswegen ist dieser Absatz ersatzlos zu streichen.	~~[2] Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen~~ ~~Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege~~ ~~sicherstellen.~~
Art. 8 Abs. 1	Aus der Formulierung dieser Bestimmung geht überhaupt nicht klar hervor, wer für die Beurteilung der Angemessenheit des Datenschutzes in einem anderen Staat zuständig ist. Aus dem erläuternden Bericht hingegen schon (S. 25 ff): Der Bundesrat ist zuständig. Der Klarheit halber sollte diese Zuständigkeit in Art. 8 E-VDSC eindeutig geregelt werden, sonst besteht das Risiko, dass sich private Akteure dafür verantwortlich halten – was ihren Aufwand erheblich erhöhen würde.	[1] Werden Personendaten ins Ausland bekanntgegeben, so müssen ~~bei der~~ anlässlich einer regelmässigen Beurteilung durch den Bundesrat, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden: […]

Art. 8 Abs. 3	Die Abstände zwischen den vorzunehmenden Beurteilungen sollen präziser angegeben werden. Deswegen wird auch hier beantragt, dass die Beurteilungen mindestens einmal jährlich stattfinden müssen.	[3] Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch, jedoch mindestens einmal pro Jahr, neu beurteilt.
Art. 9 Abs. 1	Die von Art. 9 E-VDSG gestellten Anforderungen erreichen ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Zwar sind diese Anforderungen für das Ziel des Datenschutzes konsequent, sie verursachen aber hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden. Nämlich Bst. b, c, g, h sowie i sind offensichtlich unnötig; Ihre Anwendung wäre unverhältnismässig aufwendig. Die anderen Bestimmungen genügen, um die «spezifischen Garantien» zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.	[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen die Datensicherheit mindestens die folgenden Punkte regeln: […] ~~b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen~~ ~~c. die Art und der Zweck der Bekanntgabe von Personendaten;~~ ~~[…]~~ ~~g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger;~~ ~~h. die Massnahmen zur Gewährleistung der Datensicherheit;~~ ~~i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;~~ […]

Art. 10	Wir begrüssen, dass der EDÖB eine Liste von Standard-Datenschutzklauseln veröffentlicht, um den Aufwand für die Betroffenen zu reduzieren und eine gewisse Vereinheitlichung der Schutzklauseln zu erreichen.	-
Art. 15	Bei der Anwendung dieser Bestimmung ist darauf zu achten, dass die Anforderungen an den Detaillierungsgrad der mit der Bekanntgabe von Personendaten verbundenen Informationen nicht zu umfangreich ausfallen soll. Meistens werden sich die zum Datenschutz benötigten Informationen aus den Daten oder den Begleitumständen selbst ergeben.	-
Art. 18	Nach unserer Einschätzung reicht es aus, wenn *nach Beendigung der Datenbearbeitung* (was bei entsprechenden Gerichtsverfahren bereits Jahre dauern kann) eine Aufbewahrung für ein Jahr statt zwei Jahre stattfindet.	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während ~~zwei Jahren~~ einem Jahr nach Beendigung der Datenbearbeitung aufbewahrt werden.
Art. 20	Die vorgesehene Dreifachlösung (schriftlich, mündlich oder durch Einsichtnahme an Ort und Stelle) erscheint als sehr sinnvoll. So kann für Menschen mit gewissen Krankheiten oder Beeinträchtigungen eine geeignete Lösung gefunden werden. Für gewisse Fälle, wie urteilsunfähige, an Demenz erkrankte oder weitere kognitiv behinderte Menschen dürfte die Anforderung in Abs. 3 kaum einzuhalten sein. Deshalb ist für diese Fälle eine Präzisierung aufzunehmen.	[3] Die Auskunft muss für die betroffene Person verständlich sein, soweit dies im Rahmen des kognitiven Zustands möglich ist.
Art. 22	Die Frist von 30 Tagen ab Eingang des Begehrens um Dateneinsicht erscheint uns als vernünftig. Es stellt sich einzig die Frage, ob nicht die Gerichtsferien berücksichtigt werden sollten (namentlich die Sommermonate und Weihnachten, wegen vieler Absenzen).	-
Art. 23	Bei unverhältnismässig aufwändigen Auskunftserteilungen erscheint uns die auf 300 Franken angesetzte Obergrenze als viel zu tief. Wenn damit mehrere Arbeitstage an Aufwand anfallen, wäre nicht einmal ein Bruchteil der Kosten auf die Gesuchstellenden gedeckt. Der Betrag sollte – auch gerade als Schutz vor querulatorischen Begehren – auf mindestens 1'000 Franken erhöht werden, um tatsächlich abschreckend wirken zu können.	[1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. [2] Die Beteiligung beträgt maximal ~~300~~ 1'000 Franken.

Art. 25	Die Datenschutzgesetzgebung weist eine hohe Komplexität auf; deshalb sind ihre Anforderungen in der Praxis nicht immer einfach einzuhalten. Deswegen ist es sehr sinnvoll, Datenschutzberatende einzusetzen und die konkreten Modalitäten zu deren Einsatz im Sinne dieser Bestimmung festzulegen. Die Inhalte sind zu begrüssen, wie sie in dieser Bestimmung vorgeschlagen sind.	-
Art. 26 Bst. a + b	Die hier definierte und sehr sinnvolle Ausnahme einer Pflicht zur Führung eines Bearbeitungsverzeichnisses würde bei zahlreichen Betrieben nicht zur Anwendung kommen, weil • in vielen Fällen die Betriebe besonders schützenswerte Personendaten in grossem Umfang bearbeiten; • aus einer Interpretation von Art. 20 Abs. 4, Art. 26 Abs. 3, Art. 31 Abs. 2 Bst. b nDSG hervorgeht, dass Art. 26 eVSDG auch Betriebe mit weniger als 250 Mitarbeitenden angewendet werden soll, wenn sie einem Konzern zugehören, der insgesamt mindestens 250 Mitarbeitende beschäftigt. Um Rechtssicherheit zu gewährleisten und keinen unnötigen Aufwand für kleinere Betriebe (namentlich auch gerade im Gesundheitswesen) zu schaffen, ist eine Anpassung wichtig. Während wir die Unterstellung von Teilen der Konzerne nachvollziehen können, erscheint uns die «Bearbeitung von besonders schützenswerten Daten in grossem Umfang» als zu wenig präzise Konkretisierung. Wir beantragen deshalb eine Präzisierung, was unter «grossem Umfang» zu verstehen ist, nach unserer Ansicht wäre die Schwelle etwa bei 1000 Datensätzen festzusetzen. Diesfalls erhält auch die Führung eines Verzeichnisses aber auf freiwilliger Basis mehr Gewicht, sie kann insbesondere bei regelmässiger Bearbeitung von Personendaten eine nützliche und einfache Tätigkeitsunterstützung darstellen: Dadurch können das Beibehalten eines Überblicks der Bearbeitungstätigkeiten und auch die Einhaltung anderer Verpflichtungen erleichtert werden.	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. Es werden umfangreich (mindestens 1000 Datensätze) besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.
Art. 45 Abs. 2	Aus unserer Sicht ist absolut unverständlich, warum eine nationale Behörde für die Dienstleistung im Bereich des der ganzen Bevölkerung dienenden Datenschutzes solch hohe Kostensätze von 150 bis 350 Franken verlangen soll. Dies schreckt geradezu ab, diese sinnvollen Dienstleistungen zu beziehen, welche einer guten Umsetzung der Gesetzgebung dienen. Es ist unverständlich, dass für die Dienstleistungen	[2bis] Wenn die Bearbeitung besonders schützenswerte Personendaten betrifft, wird auf die Erhebung von Kosten verzichtet. Alternativ:

	der Verwaltung solche Preise wie bei spezialisierten Anwaltskanzleien verrechnet werden. Als ganz besonders stossend empfinden wir solche Honorare zulasten von Leistungserbringern, wenn diese besonders schützenswerte Personendaten bearbeiten (dies betrifft insbesondere und in vielen Fällen die nach KVG zugelassene Leistungserbringer): Es wäre falsch, diese mit hohen Stundensätzen vom Bezug der sinnvollen Unterstützung seitens EDÖB abzuschrecken. Diese Betriebe sind denn mit den neuen Regelungen auch besonders stark herausgefordert und eine gute Umsetzung ist im Interesse der Behörden und der Bevölkerung. Diese Belastung ist umso fragwürdiger, als die öffentliche Hand im Endeffekt und in vielen Fällen, die dadurch verursachten Defizite ausgleichen soll: Mit einer Hand wegnehmen, was mit der anderen gegeben wird, macht betriebswirtschaftlich keinen Sinn und verursacht einen sinnlosen administrativen Aufwand. Die Zutrittsschwelle zum EDÖB ist niedrig zu halten, ganz besonders auch zur Überprüfung der Angemessenheit von Kodizes (Art. 59 Abs. 1 Bst. a nDSG) oder die Genehmigung von Standarddatenschutzklauseln (Art. 59 Abs. 1 Bst. b nDSG). Im Sinne einer rechtmässigen Umsetzung der komplexen neuen Datenschutzgesetzgebung sollte das Anrufen des EDÖB nicht durch das Erheben von Gebühren entgegengewirkt werden. Ganz besonders für den Bereich der Gesundheitsbetriebe muss deshalb eine Ausnahme geschaffen werden, welche vernünftige Stundenansätze vorsieht.	[2bis] Wenn die Bearbeitung besonders schützenswerte Personendaten betrifft, gilt ein Stundenansatz von 50 bis 100 Franken.

Der nationale Branchenverband CURAVIVA Schweiz bedankt sich für die ernsthafte Prüfung und Berücksichtigung der oben aufgeführten Standpunkte.

Mit freundlichen Grüssen

Laurent Wehrli
Präsident CURAVIVA Schweiz

Dr. Daniel Höchli
Direktor CURAVIVA Schweiz

Bei Rückfragen zur vorliegenden Vernehmlassungsantwort wenden Sie sich bitte an:

Yann Golay Trechsel
Projektleiter Public Affairs
E-Mail: y.golay@curaviva.ch
Tel: 031 385 33 36

Proposition d'amendement de la révision de l'ordonnance sur la protection des données

1 Contexte

L'Association Suisse pour le Label de Cybersécurité (ASLaC) réunit de multiples entités représentant les PMEs (chambres de commerce romandes, association professionnelles, etc.) et des autorités publiques (canton et union de communes). Dans le cadre des travaux de normalisation qui ont servi à déterminer les exigences du Label, nous avons eu l'occasion d'échanger abondamment au sujet du niveau de sécurité cyber des organisations de différentes tailles tout en définissant un niveau de sécurité cyber praticable. Nous avons en parallèle entrepris un grand nombre d'audits directement sur le terrain. Nous avons tiré de ces expériences une connaissance générale des besoins des petites et moyennes organisations au niveau de la sécurité cyber.

Lors de la mise en consultation de la "révision de l'ordonnance sur la protection des données" (OLPD), nous avons parcouru le document pour évaluer son impact sur les petites et moyenne organisations. Nous en avons déduit qu'au moins une modification, présentée ci-dessous, pourrait clarifier l'impact de l'ordonnance pour ce type de structures et les aider à s'y conformer.

Par le présent document nous proposons ainsi un amendement à cette ordonnance que nous vous proposons de relayer auprès de votre réseau.

2 Proposition

2.1 Amendement

Nous demandons l'adjonction du nouvel alinéa suivant à l'OLPD :

Art 26, al2.

Pour les entreprises et autres organismes déliés de l'obligation de tenir un registre des activités de traitement, l'existence de mesures de sécurité des données adaptées au risque au sens de l'art. 8 LPD peut être démontrée par la conformité à des normes ou référentiels reconnus, dont la norme ISO/CEI 27001 «Systèmes de gestion de la sécurité de l'information – Exigences » 1 ou le référentiel développé par l'Association suisse pour le label de cybersécurité.

2.2 Argumentaire

- En explicitant la non-obligation d'utilisation de normes établies (utilisation du terme «peut être démontrée»), nous éclaircissons qu'en l'absence de l'obligation de tenir un registre de traitement, une organisation peut, mais ne doit pas, démontrer l'application de mesures de sécurité relatives à leur situation. Ceci permet ainsi de faire appel à la responsabilité individuelle des organisations tout en permettant l'évolution des solutions grâces à la possibilité de les choisir librement.
- Le Label porté par l'ASLaC adopte une approche par les risques, les mesures techniques et organisationnelles exigées par notre référentiel dépendant de la valeur des données d'une organisation et des risques encourus. Le référentiel de l'ASLaC est en ce sens conforme à l'esprit de la LPD, art. 8.
- En faisant référence au Label développé par l'ASLaC, les petites et moyennes organisations, par le biais des organisations faîtières (chambre de commerce, acteurs publics, etc.), peuvent conserver une maîtrise des exigences qui font partie du référentiel utilisé par l'ordonnance. En effet, les exigences du Label sont définies sur une base participative par les membres partenaires de l'ASLaC.

- Contrairement à une partie des normes actuelles, dans lesquelles aucun niveau technique n'est en général requis, nous proposons des mesures pratiques et facilement applicables, tout en restant complètement neutres en ne proposant pas de produits et services commerciaux liés à l'implémentation de ces mesures.
- Les exigences élaborées et prochainement mises à jour pour l'ASLaC et ses membres permettent aux entreprises de définir leur niveau de risque et de déterminer les protections adaptées. Nous pensons que cette proportionnalité doit être centrale dans l'application de la sécurité cyber, afin d'éviter d'exiger des mesures de protection excessivement lourdes pour des organisations qui ne disposent ni des ressources ni des compétences nécessaires en interne.
- La démarche de l'ASLaC est reconnue au niveau national, notamment par le centre national suisse pour la cybersécurité (NCSC), qui y fait référence dans ses différents rapports : « Initiative privée développée en étroite collaboration avec des représentants des PME, le label (…) contribue fortement à la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC).» (Le Conseil fédéral, Rapport de mise en œuvre de la SNPC, 2020).

datenschutzguide.ch GmbH, Hegibachstr. 47, 8032 Zürich

Per E-Mail an
Jonas.amstutz@bj.admin.ch

Zürich, den 13. Oktober 2021

Vernehmlassung VDSG

Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir von der datenschutzguide.ch GmbH sind ein interdisziplinäres Datenschutz-Team bestehend aus praxiserprobten Telekommunikations-, IT-, Datenschutz- und Technologierechtsspezialisten.

Diese Eingabe erfolgt unabhängig eines konkreten Mandates und beschränkt sich auf die nachfolgend als wesentlich erachteten Punkte, die einer Änderung bedürfen. Wir verzichten darauf, die zahlreichen positiven Aspekte (bspw. risikobasierter Ansatz) hervorzuheben.

Als Vorbemerkung drängen sich einige Hinweise zum formellen Legalitätsprinzip auf:

Anders als das materielle Legalitätsprinzip, welches seine Grundlage in Art. 5 Abs. 1 BV hat, stützt sich das formelle Legalitätsprinzip für die Bundesebene auf Art. 164 und Art. 182 BV, wonach alle wichtigen Rechtssätze in Form des Bundesgesetzes, d.h. durch das Parlament unter Referendumsvorbehalt, zu erlassen sind. Der demokratische Aspekt des Legalitätsprinzips wird damit durch die Beachtung der Rechte von Parlament und Stimmvolk gesichert. Das Demokratieprinzip schweizerischer Konzeption besagt, dass wichtige Entscheide vom Parlament und/oder direkt vom Stimmvolk zu fällen sind, weshalb in Bezug auf den formellen Aspekt des Legalitätsprinzips auch von einem Parlaments- bzw. Volksvorbehalt gesprochen wird. Wichtige Bestimmungen müssen deshalb das formelle Gesetzgebungsverfahren durchlaufen haben; es besteht insofern ein Gesetzesvorbehalt im Sinne eines Vorbehalts des formellen Gesetzes. In diesem Sinne muss der Gesetzgeber nach der sog. Wesentlichkeitstheorie das Wichtige selber festlegen. **Namentlich die Auferlegung von Leistungspflichten, wie auch die Festlegung der Rechte und Pflichten unter Privaten, bedürfen eines Entscheides durch den Gesetzgeber**. Die Verordnungsstufe genügt hierfür nicht (aus Stauffer von May Nando, Regionale Aufgabenerfüllung und demokratische Rechte, Diss. Bern 2018, N 182-192).

Nicht wichtige Aspekte, darf der Gesetzgeber an den Verordnungsgeber delegieren. Die herrschende Lehre und Rechtsprechung verlangen grundsätzlich eine **explizite Delegationsnorm**, wobei zwischen gesetzesvollziehenden Verordnungen, zu deren Erlass die

Exekutive regelmässig bereits von Verfassung wegen zuständig ist und gesetzesvertretenden Verordnungen unterschieden wird, welche einer expliziten Regelung im formellen Gesetz bedürfen. Die explizite Delegationsbestimmung soll dabei verdeutlichen, wo der Gesetzgeber mit der eigenen Legiferierung aufhört und ab wann er eine Regelung nicht mehr für wichtig erachtet und dem Verordnungsgeber überlassen will (Stauffer von May Nando, Regionale Aufgabenerfüllung und demokratische Rechte, Diss. Bern 2018, N 202).

Vor dem Hintergrund des Vorstehenden ist es unzulässig, in der Verordnung Privaten wesentliche neue Pflichten aufzuerlegen, die im nDSG nicht vorgesehen sind. Ebenso unzulässig ist es, gänzlich ohne Delegationsnorm Regeln zu erlassen. Entsprechend sind folgende Artikel aus der Verordnung zu entfernen bzw. ggf. anzupassen:

Art. 2 Schutzziele: Die Festlegung von umfassenden Schutzzielen ist u.E. von der Delegationsnorm, Art. 8 Abs. 3 nDSG, nicht mehr gedeckt. Die Verordnung soll bloss Mindestanforderungen an die Datensicherheit festlegen. Inhaltlich ist im Übrigen anzumerken, dass die zwei einleitenden Wörter «soweit angemessen» zentral sind. In der Tat ist die Umsetzung vieler der in Art. 2 VDSG genannten Schutzziele für KMUs nur bedingt angemessen. Es stellt sich die Frage, wer über die Angemessenheit entscheidet. Dies ist insbesondere im Hinblick auf die Strafbarkeit nach Art. 61 lit. c nDSG von Bedeutung. Unseres Erachtens sollte sich der Gesetz- und Verordnungsgeber auf minimale Vorschriften beschränken und keinen detaillierten Schutzzielekatalog festlegen. Es wäre auch etwas mehr Vertrauen in die Marktkräfte und das neue DSG angezeigt. Kein Unternehmen wünscht sich eine Meldung wegen Verletzung der Datensicherheit. Auch erhalten Unternehmen, welche den Datenschutz (inkl. Datensicherheit) im Griff haben, in der Regel bspw. bessere Konditionen bei Cyber-Versicherungen. Auch verlangen Auftraggeber von Beauftragten immer häufiger eine Kopie der *IT-Security Policy*. Es gibt daher bereits genügend Anreize, die Datensicherheit ernst zu nehmen. Ein detaillierter und überdies vor allem strafbewährter Katalog ist unseres Erachtens nicht angebracht.

Art. 3 Protokollierung: Diese Pflicht geht u.E. über die Mindestanforderung an die Datensicherheit hinaus (s.a. S. 20 des erläuternden Berichts, wonach die Protokollierung nur im Nachgang zu einer Verletzung der Datensicherheit dienlich ist); weshalb es an einer genügenden Delegationsnorm mangelt.

Art. 4 Bearbeitungsreglement von privaten Personen: Diese erhebliche Pflicht bedürfte einer expliziten Regelung im formellen Gesetz. Überdies ist die Pflicht zur Führung eines Bearbeitungsreglements nebst dem Bearbeitungsverzeichnis auch inhaltlich verfehlt und längst nicht mehr von der Delegationsnorm von Art. 8 Abs. 3 nDSG gedeckt.

Art. 5 Bearbeitungsreglement von Bundesorganen: s.o.

Art. 9 Datenschutzklauseln und spezifische Garantien: Es fehlt eine Delegationsnorm. Im Übrigen ist bei der Verwendung von Datenschutzklauseln Mitteilung an den EDÖB zu machen, was u.E. eher dafür spricht, dass dieser hierzu allenfalls ein Merkblatt erlässt. Es fehlt an der Regelungskompetenz des Verordnungsgebers und überdies auch am Regulierungsbedarf.

Art. 13 Abs. 2 Piktogramme: Es fehlt eine Delegationsnorm und auch die Notwendigkeit einer Regulierung ist nicht ersichtlich.

Art. 15 und 16 neue Informationspflichten: Diese zusätzlichen Informationspflichten sind ohne jegliche gesetzliche Grundlage oder Delegationsnorm klarerweise unzulässig.

Art. 20 Abs. 5 (und auch der diesbezügliche Verweis in Art. 24) Dokumentationspflicht: Es fehlt wiederum an einer Delegationsnorm und überdies auch an einer Regulierungsnotwendigkeit.

Sodann würden wir anregen, folgende Versehen zu korrigieren:

Art. 6 Abs. 3 sowie **Art. 18** sprechen von «**schriftlich**», während der erläuternde Bericht (S. 35) festhält, dass auch elektronisch ausreichend sei. Letzteres erfüllt die Kriterien der Schriftlichkeit allerdings nur, wenn das elektronische Dokument mit einer qualifizierten elektronischen Signatur signiert wird. Dies scheint uns unnötig und praxisfremd. Anstelle der Schriftlichkeit sollte der Nachweis in Textform ausreichend sein.

Art. 13 Abs. 1: Den Auftragsbearbeiter trifft – soweit er als Auftragsbearbeiter tätig ist – keine Informationspflicht. Dort wo der Auftragsbearbeiter selber als Verantwortlicher gilt, bspw. in Bezug auf Mitarbeiter, trifft ihn freilich eine Informationspflicht. Da der Auftragsbearbeiter diesbezüglich aber als Verantwortlicher gilt, ist der Auftragsbearbeiter in Art. 13 nicht mehr zu erwähnen.

Mit freundlichen Grüssen

datenschutzguide.ch GmbH

Dr. Nando Stauffer von May *Marco Novoselac*

Datenschutz Forum Schweiz

Zürich, 12. Oktober 2021

Bundesamt für Justiz
Direktionsbereich Öffentliches Recht
Bundesrain 20
3003 Bern

Vernehmlassung zur Totalrevision der

Verordnung zum BG über den Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Das Datenschutz-Forum Schweiz wurde im September 1999 als Verein mit dem Zweck gegründet, die praktische Umsetzung sowie die Forschung auf dem Gebiet des Datenschutzes und der Datensicherheit zu fördern. Seit nunmehr 22 Jahren geschieht dies insbesondere durch den Informations- und Erfahrungsaustausch unter den am Datenschutz interessierten Personen aus allen Fachrichtungen der Wirtschaft, der öffentlichen Verwaltung und der Wissenschaft.

Für betroffene Personen, Datenbearbeitenden, Behörden, Politiker und Medien stellt das Datenschutz-Forum Schweiz Informationen sowie Unterlagen für die Meinungs- und Entscheidungsfindung in Datenschutz- und Datensicherheitsfragen zur Verfügung. Es fördert die Aus- und Weiterbildung auf diesem Gebiet und pflegt Kontakte zu Organisationen mit gleichen Zielsetzungen.

Vor diesem Hintergrund nehmen wir gerne die Gelegenheit wahr, uns am Vernehmlassungsverfahren zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz zu beteiligen und dazu Stellung zu nehmen. Das Datenschutz-Forum Schweiz hat sich bei seinen Bemerkungen v.a. auf Grundlegendes im Vorentwurf beschränkt oder sich auf Normen konzentriert, welche erheblich nachbesserungsfähig sind. Die Vorlage hat insgesamt gelungene Vorschläge wie eine bessere Systematik, insgesamt erscheint sie aber leider noch zu unausgereift und zahlreiche Bestimmungen sind losgelöst von den gesetzlichen Grundlagen im nDSG und auch von der DSGVO. Aus Kapazitätsgründen konnten wir diese nicht alle in unserer Vernehmlassung thematisierten.

1. Allgemeines

Die Verordnungsartikel sind vom Wortlaut her häufig aus sich heraus nicht gut verständlich, sondern benötigen den „Erläuternden Bericht zur Revision der Verordnung zum BG über den Datenschutz". Dies ist insofern bedauerlich, da damit zu rechnen ist, dass Verantwortliche von personenbezogenen Datenbearbeitungen sich lediglich am Gesetzes- und Verordnungstext orientieren. Deshalb schlagen wir generell vor, dass der Verordnungstext sprachlich präziser gestaltet wird, dabei teilweise auch mit Beispielen zur besseren Verständlichkeit gearbeitet wird oder auch nochmals Bezug auf den Gesetzestext genommen wird. Wir vermissen im Entwurf die durchgehende Berücksichtigung des Leitfadens zur geschlechterneutralen Formulierung:
(s.https://www.bk.admin.ch/bk/de/home/dokumentation/sprachen/hilfsmittel-textredaktion/leitfaden-zum-geschlechtergerechten-formulieren.html).
Wir würden es begrüssen, wenn bei den «einleitenden» Allgemeinen Bestimmungen die Verantwortlichen und Auftragsbearbeitenden als Hauptadressaten der meisten Normen häufiger genannt werden würden, damit sich diese ihrer umfangreichen Verantwortung bewusst sind.

2. Stellungnahmen zu einzelnen Normen

Art. 1 E-VDSG (Grundsätze) Für Art. 1 E-VDSG wurde Art. 8 Abs. 1 nDSG übernommen, aber durch eine geänderte Satzstellungen und Hinzufügungen hat die Norm in ihrer Aussagekraft bzw. in ihrer Verständlichkeit gelitten. Hier schlagen wir vor, Verantwortliche und Auftragsbearbeitende wieder namentlich aufzuführen (vgl. unsere Bemerkungen unter «1. Allgemeines»). Unser Vorschlag wäre, Art. 8 Abs. 1 nDSG als klar verständlichen Einleitungssatz zu übernehmen. Wir sind uns bewusst, dass eine Wiederholung des Textes auf Verordnungsebene in der Regel redaktionell unerwünscht ist. Aber wir betrachten eine Wiederholung eines klaren Gesetzestextes als weniger problematisch als eine Grundsatznorm, die mit dem Wort «Ob» beginnt.
Im zweiten Satz können dann die Kriterien folgen. Hier sollte das Wort «insbesondere» einfliessen, damit den Normadressaten klar wird, dass diese nicht vollständig aufgelistet sind. Es finden sich in Art. 8 Abs. 1 nDSG keine Hinweise darauf, dass der Gesetzgeber die Kriterien begrenzen wollte und eine solche Begrenzung ist u.E. auch nicht sinnvoll.

Dadurch kann auch auf den Begriff «Umstände» in Abs. 1 Bst. c E-VDSG verzichtet werden, da dieser als Ergänzung falsch gewählt worden ist, um künstliche Intelligenz als besonders hohes Risiko einer automatisierten Datenbearbeitung aufzuführen. Erstens ist er bereits in der «Art» der Datenbearbeitung erfasst, und zweitens entsteht der Eindruck, dass noch rasch der Entwurf der EU-Kommission für eine KI-Verordnung in der Vorlage berücksichtigt werden sollte. Es wäre aus unserer Sicht wün

schenswert, wenn die datenschutzrechtliche Auseinandersetzung mit der möglichen Normierung von KI-Technologien gründlicher erfolgt.

Unser Änderungsvorschlag:

Art. 1 Grundsätze

[1] Der Verantwortliche und der Auftragbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit. Dies beurteilt sich insbesondere nach den folgenden Kriterien:

a. Zweck, Art und Umfang der Datenbearbeitung;…

Art. 2 E-VDSG (Schutzziele): Als redaktionellen Vorschlag empfehlen wir Ihnen, den Einleitungssatz der Norm umzustellen: In seiner jetzigen Form kann der Sinn der Angemessenheit falsch verstanden werden. Wir weisen in diesem Zusammenhang auf den DSG-Kurzkommentar von Bruno Baeriswyl zu Art. 7 hin (S. 92 ff.).

Zudem ist eine abschliessende Auflistung von Schutzzielen nicht zielführend, da es sich bei der anschliessenden Auflistung nicht um Schutzziele handelt, sondern um technische und organisatorische Massnahmen, welche die Datensicherheit bei der Bearbeitung personenbezogener Daten beinhaltet. Hier ist für uns nicht nachvollziehbar, dass gemäss „Erläuterndem Bericht" grösstenteils Art. 9 VDSG übernommen wurde, der bereits seit Jahren als antiquiert gilt. Wir vertreten die Ansicht, dass die nicht abschliessend (vgl. unsere Bemerkung zu Art. 1 E-VDGS) aufgezählten Massnahmen, die zum angestrebten Schutzziel lenken, gemeinsam mit Informatik- und Datenschutzexpert:innen nochmals überprüft und bereinigt werden. Dabei wären auch die DSGVO und internationale Standards als Materialien beizuziehen. Wir schlagen bei diesen vor, auf absolute Verben wie «verunmöglichen» (Art. 2 Abs. 2 Bst. c) zu verzichten und eher Verben wie «sicherzustellen» einzusetzen.

Der Katalog der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden, womit die Liste auch mit Art. 32 DSGVO konform wäre.

Diese Massnahmen sind natürlich zu trennen von technischen und organisatorischen Bestimmungen, welche den Schutz der Rechtmässigkeit der Verarbeitung beinhalten (unterschiedlicher Gegenstand).

Unser Änderungsvorschlag:

Art. 2 Schutzziel

Die Verantwortlichen müssen dafür sorgen, dass alle notwendigen Massnahmen zur Datensicherheit getroffen werden, damit ein angemessener Schutz derjenigen Personen gewährleistet ist, deren Daten sie bearbeiten. Dazu zählen namentlich: .....

Art. 3 E-VDSG (Protokollierung): Der Begriff «private Verantwortliche» wird in Absatz 1 eingeführt. Dies irritiert, da diese Bezeichnung nicht in Art. 5 nDSG erklärt wird, und es somit an der notwendigen gesetzlichen Grundlage fehlt, weshalb alternativ überlegt werden muss, ob dieser Artikel allenfalls auch zu streichen ist. Zudem wird es in den wenigsten Betrieben die Aufgabe des «Verantwortlichen» sein, zu protokollieren. Vielmehr hat er (oder sie) dafür zu sorgen, dass protokolliert wird. Der Auftraggeber ist sowieso verpflichtet, zu protokollieren, falls dies zu den Pflichten des Verantwortlichen gehört.

Das Wort «zumindest» beinhaltet eine Wertung in der Norm, die jedoch keine Rechtsfolge auslöst, dementsprechend kann auf dieses Wort in den Absätzen 1 und 2 verzichtet werden.

Absatz 4: Hier fragen wir uns, ob der Ausdruck «für diesen Zweck» inhaltlich korrekt ist.

Unser Änderungsvorschlag:

Art. 3 Protokollierung *[1] …, sorgt der Verantwortliche einer privaten Person dafür, dass folgende Vorgänge protokolliert werden:…* *[4]* …, und dürfen nur im Rahmen dieser Aufgabenerfüllung bearbeitet werden *Alternativ: Artikel streichen*

Art. 4 E-VDSG (Bearbeitungsreglement von privaten Personen): Die Verknüpfungen von Datenbeständen gehören zu den grössten Risiken für die Datensicherheit im Betrieb. Dementsprechend sollte das Bearbeitungsreglement von privaten Personen auch solche Verknüpfungen aufführen. Auch hier fehlt es an der notwendigen Grundlage, und das Verhältnis zum Bearbeitungsverzeichnis (BV) ist unklar und redundant, weshalb alternativ diese Bestimmung auch gestrichen werden kann.

Art. 5 E-VDSG (Bearbeitungsreglement von Bundesorganen): Die Regelung ist einerseits unverhältnismässig, andererseits fehlt es an der entsprechenden gesetzlichen Grundlage, weshalb der Artikel zu streichen ist.

Art. 6 E-VDSG (Modalitäten): Sprachlicher Verbesserungsvorschlag:
Der Verantwortliche kann nicht sicherstellen, sondern lediglich für die vertrags- und gesetzesmässige Bearbeitung sorgen. Auch ist die Form der Zustimmung unklar formuliert.

Unser Änderungsvorschlag:

Art. 6 Modalitäten *[2] Untersteht der Auftragbearbeiter nicht dem DSG,… .... die Zustimmung erfolgt schriftlich oder in elektronischer Form.....*

Art. 7 E-VDSG (Informationen an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans): Art. 7 stützt sich auf Art. 9 nDSG ab. Hier hat der Bundesrat relativ viel Gestaltungsraum, wie Datenschutzberatende einzubeziehen sind. In der Praxis ist es wesentlich effektiver, wenn

Datenschutzberatende vorgängig in solche Projekte einbezogen werden. Dadurch kann das Fachwissen bereits bei der Projektplanung einbezogen werden, damit sie ihre Beratungsfunktion erfüllen können. Datenschutzbeauftragte sind sinnvollerweise vor allem präventiv aktiv und dies sollte bei der Ausgestaltung dieses Artikels unbedingt berücksichtigt werden, damit nachfolgende Probleme bei der Einhaltung von Datenschutzvorschriften soweit wie möglich vermieden werden können. Dies kann im Rahmen einer vorgängigen Konsultation der datenschutzbeauftragten Person geschehen, wobei auch der Einsitz in entsprechende Gremien dazu zählt. Hier verweisen wir auch auf die Leitgedanken zur Revision des DSG (vgl. u.a. 17.059 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, S. 6943).

Art. 9 E-VDSG (Datenschutzklauseln und spezifische Garantien): Der Anforderungskatalog ist entweder zu streichen oder dann entsprechend anzupassen, indem „mindestens“ durch „je nach den Umständen“ zu ersetzen ist.

Art. 13 E-VDSG (Modalitäten der Informationspflichten): Auch hier fehlt es an der entsprechenden gesetzlichen Grundlage, indem das nDSG keine Informationspflicht des „Auftragsbearbeiter“ vorsieht. Die Regelung betreffend Piktogramme macht nicht wirklich Sinn und kann sogar zu Rechtsunsicherheit führen, weshalb der Artikel zu streichen ist.

Art. 15 E-VDSG (Information bei der Bekanntgabe von Personendaten): Für die darin vorgesehene Informationspflicht für die Verantwortlichen und Auftragsbearbeiter fehlt es an der gesetzlichen Grundlage, und die Bestimmung ist in dieser Form kaum praktikabel, weshalb sie entweder für private Datenbearbeiter anzupassen oder ganz zu streichen ist.

Art. 16 E-VDSG (Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten): Auch hier fehlt es an der entsprechenden gesetzlichen Grundlage im nDSG, weshalb der Artikel gestrichen werden sollte.

Art. 17 E-VDSG (Überprüfung einer automatisierten Einzelentscheidung): Diese Norm beruht auf dem ausführlichen Art. 21 nDSG. Sie will verhindern, dass betroffene Personen, die ihre gesetzlichen Rechte wahrnehmen, nicht benachteiligt werden. Es fragt sich jedoch, was mögliche Benachteiligungen sein könnten? Hier wäre die Auflistung von konkreten Beispielen hilfreich.

Art. 18 E-VDSG (Form und Aufbewahrung der Datenschutz-Folgeabschätzung): Die Datenschutz-Folgeabschätzung ist ein äusserst sinnvolles Instrument zur systematischen Risikoeindämmung und stellt eine der wichtigsten Neuerungen des nDSG dar. Falls sich aus einer missbräuchlichen Datenbearbeitung Schäden für die betroffene Person ergeben und sich in der Folge Haftungsfragen stellen, kann die Datenschutz-Folgeabschätzung als Dokument dazu dienen, entsprechende Haftungsansprüche zu prüfen. Dementsprechend sollte die Aufbewahrungsfrist auf fünf Jahre verlängert werden. Zudem sollte „Schriftlichkeit" angepasst werden mit „in geeigneter Weise" oder „in Textform".

Art. 19 Abs. 5 E-VDSG (Meldung von Verletzungen der Datensicherheit): Die Dokumentation des EDÖB kann im Falle von Haftungsansprüchen relevant sein; eine Aufbewahrungsfrist von drei Jahren ist zu kurz und sollte auf fünf Jahre verlängert werden (s. auch Bemerkung zu Art. 18 E-VDSG).

Art. 20 E-VDSG (Modalitäten): Die Modalitäten zum Auskunftsbegehren sollten so geregelt werden, dass es problemlos für die betroffene Person ist, ihr Auskunftsrecht in angemessenen Abständen wahrzunehmen. Weiter wichtig ist, dass dieses Instrument nicht zum Rechtsmissbrauch benutzt wird.

Die Auskunft kann wiederum als Dokument bei Haftungsfragen dienen und die Auskunftspflicht sollte deshalb auf fünf Jahre verlängert werden (s. auch Bemerkung zu Art. 18 E-VDSG). Zudem sollte die Auskunft „im Grundsatz nachvollziehbar sein", und zwar nicht nur für die betroffene Person.

Art. 21 E-VDSG (Zuständigkeit): Es stellt sich die Frage, wie die Auskunft erfolgt, wenn mehrere Verantwortliche gemeinsam die Daten bearbeitet haben. Abgrenzungsschwierigkeiten sind ein bekanntes Problem zwischen gemeinsamen Verantwortlichen; dementsprechend wäre es sinnvoll, ein Regelwerk zu erarbeiten, welches verhindert, dass der betroffenen Person aus dieser Konstellation Nachteile erwachsen, wie beispielsweise ein Herumgeschiebe der Verantwortlichkeiten oder eine lückenhafte Auskunft. Es sollte deshalb präzisiert werden: „Sind für die Bearbeitung von Personendaten mehrere *gemeinsam* verantwortlich....".

Art. 25 E-VDSG (Datenschutzberaterin oder Datenschutzberater): Der Aufgabenbereich für Datenschutzberater, resp. Datenschutzberaterinnen ist rudimentär normiert. Hier sollte neben der Erwähnung der Mitwirkung an der Datenschutz-Folgenabschätzung die datenschutzfördernden Aufgaben der Datenschutzbeauftragten Person bei privaten Organisationen und Unternehmen thematisiert werden, beispielsweise im Sinne einer Obliegenheit. Wie bereits unter Art. 7 E-VDSG erwähnt, sollten Datenschutzberatende vermehrt präventiv tätig sein, sei es bei der Implementierung eines Datenschutz-Management-Systems, bei der Anschaffung neuer IT-Systeme oder bei der Schulung des Personals. Es empfiehlt sich deshalb, die Aufgaben der Datenschutzberaterin oder des Datenschutzberaters genauer zu präzisieren.

Art. 31 E-VDSG: Der Begriff „sogleich" ist zu ungenau und sollte durch „rechtzeitig" ersetzt werden.

Art. 32 E-VDSG: Abgesehen davon, dass Meldungspflichten in der Regel vor allem einen bürokratischen Mehraufwand ohne entsprechenden Nutzen für die Betroffenen bedeuten, sollte diese Bestimmung aufgrund der fehlenden gesetzlichen Grundlage gestrichen werden.

Art. 39 E-VDSG (Mitteilung von Richtlinien und Entscheiden): Es stellt sich die Frage, weshalb die Bundesverwaltung ihre Richtlinien dem EDÖB in anonymisierter Form mitzuteilen hat (vgl. Absatz 1).

Richtlinien zum Datenschutzgesetz sind Rahmenbedingungen, die an mehrere Adressaten gerichtet werden und diese sollten in der Regel dem Öffentlichkeitsprinzip unterstellt sein. Aus dem bisherigen Art. 32 Abs. 2 zweiter Satz VDSG lässt sich u.E. nach Wortlaut und Satzstellung nur ableiten, dass Entscheide in anonymisierter Form dem EDÖB mitzuteilen sind.

Wie bereits eingehend erwähnt, sollte eine Verordnung die im entsprechenden Gesetz geregelten Grundsätze praxisbezogen präzisieren und nicht losgelöst davon neue Grundsätze definieren, was leider in der E-VDSG nicht konsequent erfolgt ist. Auch wäre es für die mit der Umsetzung in der Praxis Betroffenen sinnvoll und hilfreich, wenn die Bestimmungen nicht allzu weit von der auch in der Schweiz oft geltenden DSGVO abweichen würden.

Im Namen des Datenschutz-Vorstands

Cordula E. Niklaus, Co-Präsidentin

Die Schweizerische Post AG
Stab CEO
Wankdorfallee 4
3030 Bern

www.post.ch

Die Schweizerische Post AG, Stab CEO, Wankdorfallee 4, 3030 Bern

Eidg. Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

Als Word/PDF an: jonas.amstutz@bj.admin.ch

Datum 12. Oktober 2021
Ihre Nachricht Stellungnahme VE-VDSG
Kontaktperson Gabriele Schmid-Strasser
E-Mail gabriele.schmid@post.ch
Direktwahl +41 58 386 66 62

Stellungnahme der Schweizerischen Post zum Vorentwurf zu der totalrevidierten Verordnung zum Bundesgesetz über den Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, im Rahmen der Vernehmlassung zu der totalrevidierten Verordnung zum Bundesgesetz über den Datenschutz Stellung zu nehmen.

1. Ausgangslage für die Schweizerische Post

Die Post sieht in der digitalen Transformation grosse Chancen für die Schweiz. Auf Basis ihrer neuen Strategie «Post von morgen» erfüllt die Post als Motor für eine moderne Schweiz auch die neuen Bedürfnisse unserer Kundinnen und Kunden, ganz gleich ob physisch oder digital.

Die Anforderungen an Vertraulichkeit und Privatsphäre im Umgang mit sensiblen Informationen und Daten gewinnen stärker an Bedeutung. Der verantwortungsvolle Umgang mit Daten ist ein zentraler Wert der Schweizerischen Post. Interaktion – einfach, sicher, digital: Wir wollen das bewährte Prinzip des Briefgeheimnisses auch in der digitalen Welt sicherstellen, darum erweitern wir unser Portfolio mit neuen digitalen Leistungen und bauen dabei auf unserer langjährigen Erfahrung als vertrauenswürdige Übermittlerin von schützenswerten Informationen auf. Die Post ist bestrebt, mit ihren Dienstleistungen und Angeboten die Digitalisierung breit in die Bevölkerung und in die Wirtschaft zu tragen.

Klara, eine Konzerngesellschaft der Post, bietet umfassende digitale Lösungen für KMU an, um deren administrativen Alltag zu entlasten. Bund und Kantonen bietet die Post zahlreiche Dienstleistungen im Bereich der digitalen Verwaltung. Zu nennen sind beispielsweise E-Voting, IncaMail, elektronisches Patientendossier (EPD) und elektronischer Betreibungsregisterauszug. Zwischen Privaten und Behörden sowie unter Behörden ganz gleich ob physisch oder digital spielt die Schweizerische Post eine zentrale Rolle als vertrauenswürdiger Kommunikationskanal. Das neue Datenschutzgesetz sowie die Ausführungsbestimmungen in der Verordnung sind daher für die digitale Transformation bei der Schweizerischen Post und ihren Konzerngesellschaften von grosser Bedeutung.

Auf die Schweizerische Post sind primär die Bestimmungen für Privatpersonen anwendbar. Im Rahmen der laufenden Revision zum Bundesgesetz über die Personenbeförderung («Reform des regionalen Personenverkehrs») werden Datenbearbeitungen im Zusammenhang mit Mobilitätsangebote teilweise den Datenschutzbestimmungen der Bundesorgane (Art. 54 Abs. 5 revPBG) unterstellt. Nebst PostAuto AG wäre auch die Schweizerische Post AG als Auftragsbearbeiterin der PostAuto AG von den Bestimmungen der Bundesorgane betroffen. Unsere nachfolgenden Ausführungen beziehen sich daher sowohl auf die Bestimmungen für Privatpersonen, wie auch für Bundesorgane.

2. Grundsätzliches zum Entwurf

Wir ***verstehen den durch die Gesetzesrevision gestärkten Datenschutz als Entwicklungschance in der digitalen Transformation***. Um dieses Ziel zu erreichen, bedarf es klarer Regelungen, welche den Fokus auf den Persönlichkeitsschutz der betroffenen Personen legen. Begrüssenswert wäre daher die Überprüfung derjenigen Verordnungsbestimmungen mit hohem Detailierungsgrad oder Fokus auf administrative Themen, um die Vielfalt von Datenbearbeitungen mit zu berücksichtigen und eine rechtsgenügliche Umsetzung zu konkretisieren. Zudem ist zu beachten, dass sich die Technologie rasant weiterentwickelt. Diesem Umstand ist insbesondere bei den Bestimmungen zur Datensicherheit mit einer genügend offenen Formulierung zu begegnen.

Die Umsetzungsvorgaben der Verordnung müssen ***im Rahmen des bereits verabschiedeten Bundesgesetzes bleiben***. Zahlreiche Bestimmungen des VE-VDSG sind jedoch ohne gesetzliche Grundlage und gehen über das nDSG hinaus. Diese Bestimmungen sind hinsichtlich ihres Regelungsgehalts für die Aufnahme in eine Vollziehungsverordnung ungeeignet. Die Bestimmungen ohne gesetzliche Grundlage erlegen zudem den Datenbearbeitern Pflichten auf, die mit grossen finanziellen Auswirkungen verbunden sind, eine kritische Intensität der Regelung überschreiten und in der Praxis kaum umsetzbar scheinen. Wir sind überzeugt, dass diese neuen, im Gesetz nicht vorgesehenen Pflichten keinen erwähnenswerten Mehrwert liefern, im Gegenteil sogar zu einer grossen Rechtsunsicherheit führen. Zudem hat die Schweizerische Post bereits vor Monaten, basierend auf dem vom Parlament verabschiedeten Gesetzesentwurf mit der Umsetzung begonnen, da das Gesetz keine Übergangsfristen vorsieht. Sollen diese neuen Pflichten über die Verordnung adressiert werden, bedarf es zumindest eine angemessene Übergangsfrist um die neuen Pflichten ebenfalls fristgerecht umsetzen zu können.

Ohne erkennbaren Grund führt der Bundesrat auf Verordnungsebene verschiedene «Swiss Finishes» ein. Dem anspruchsvollen gesetzgeberischen Prozess und Anliegen um eine massvolle und der europäischen Regelung äquivalente Datenschutzgesetzgebung wird damit keine Sorge getragen. Für Schweizer Unternehmen würden die Swiss Finishes zu wesentlichen Wettbewerbsnachteilen führen.

Einige Formulierungen des VE-VDSG sind zu wenig präzise. Hinzukommt ein Erläuterungsbericht, der in direktem Widerspruch zum Wortlaut des VE-VDSG steht und mit Beispielen argumentiert, die nicht verallgemeinerungswürdig sind. Auch der risikobasierte Ansatz des nDSG ist im VE-VDSG nicht mehr erkennbar. Dadurch verliert der VE-VDSG an Lenkungskraft, zumal angesichts der Komplexität des Regelungsgegenstands die zu erreichenden Ziele nicht verdeutlicht werden. Namentlich bei der Fortführung unbestimmter Rechtsbegriffe besteht ein Nachbesserungsbedarf.

Der VE-VDSG unterstützt das Ziel des Bundesrates nicht, die Schweiz zum führenden digitalen Innovations- und Wirtschaftsstandort weiterzuentwickeln. Insbesondere auch deshalb nicht, weil eine grosse Anzahl von Pflichten mit strafrechtlichen Sanktionen bedroht ist. Die digitale Transformation der Schweiz hängt zu einem grossen Teil von der Innovationskraft der Unternehmen ab. Die Datenschutzgesetzgebung der Schweiz darf dies nicht verhindern, sofern man künftig nicht ausschliesslich auf ausländische digitale Lösungen setzen will.

3. Im Einzelnen

Artikel 1 Absatz 1
Grundsätzlich wird begrüsst, dass bei der Datensicherheit dem risikobasierten Ansatz Rechnung getragen werden soll. Wir empfehlen jedoch eine Präzisierung der Terminologie. Massnahmen zur Datensicherheit müssen grundsätzlich «geeignet» (Art. 8 Abs. 1 nDSG) und nicht «angemessen» sein. Art. 1 Abs. 1 lit. d VE-VDSG benennt Implementierungskosten als eines von vier Beurteilungskriterien der Angemessenheit technischer und organisatorischer Massnahmen. Die Schweizerische Post AG regt aus folgenden Gründen an, auf eine betriebswirtschaftliche Betrachtung der Aufwände anstelle der Implementierungskosten von Schutzmassnahmen abzustellen.

- Für Verantwortliche sind neben dem initialen Kostenblock bei der Implementierung auch langfristige Betriebskosten (Personal, Lizenz, Wartung, etc.) und weitere quantifizierbare Aufwände wie Schulungen relevant. Die risikoorientierte Betrachtung lässt gerade eine umfassende, betriebswirtschaftliche Beurteilung der Eignung von Schutzmassnahmen zu.
- Im Widerspruch zum Wortlaut setzt der Erläuterungsbericht einen reduzierten Beurteilungsmassstab nach den Kriterien in Art. 1 Abs. 1 lit. a - c VE-VDSG fest; die Implementierungskosten kommen bloss als Auswahlkriterium bei nach Art. 1 Abs. 1 lit. a - c VE-VDSG gleichwertigen Massnahmen zur Anwendung (Erläuterungsbericht, S. 16). Eine Kaskadierung ist dem VE-VDSG nicht zu entnehmen, weshalb die Auslegung contra legem im Erläuterungsbericht unverständlich ist.
- Es ergibt sich bereits aus dem allgemeinen Verhältnismässigkeitsprinzip, dass der Verantwortliche die kostengünstigere Variante innerhalb einer Auswahl von Massnahmen auswählen kann, dies braucht deshalb nicht ausdrücklich erwähnt zu werden.

Statt von «angemessenen» Massnahmen ist von «geeigneten» Massnahmen zu sprechen. *«Implementierungkosten» in Artikel 1 Absatz 1 Lit. d ist durch «Aufwand» zu ersetzen.*

Artikel 1 Absatz 2
Die Besonderheiten des Einzelfalles sind ausschlaggebend, ob eine Überprüfung der TOM stattfinden soll und wie die Zeitabstände zu definieren sind. Ändert sich an einer konkreten Datenbearbeitung nichts Wesentliches, so kommen auch keine neuen Risiken hinzu. Ist dagegen von einer Gefährdung der Rechte von Betroffenen auszugehen, so ist der zeitliche Abstand selbstverständlich kürzer. Daher regen wir zur Überprüfung der Regelung an, um einen unverhältnismässigen Prüfaufwand ohne erkennbaren sachlichen Grund bei Unternehmen zu vermeiden.

«in angemessenen Abständen» in Artikel 1 Absatz 2 ist deshalb zu streichen. Eventualiter ist «angemessene Abstände» durch «angemessene Weise» zu ersetzen.

Artikel 2
Der Katalog der Schutzziele ist zu detailliert, absolut und extensiv. Im Sinne der angestrebten Europa-Kompatibilität wäre die Begrenzung auf die in Art. 32 Abs. 1 lit. b DSGVO aufgeführten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit begrüssenswert. Zudem ist die Formulierung von Art. 2 VE-VDSG in doppelter Hinsicht unklar. Mit der Muss-Formulierung («*müssen* die Massnahmen [...] folgende Schutzziele erreichen») ist eine starre Einhaltung sämtlicher Schutzziele je Massnahme suggeriert. Zudem wird mit «[...] Schutzziele *erreichen*» der verordnete Schutz verabsolutiert. Insofern werden Maximalanforderungen formuliert, was wir mit Blick auf die Strafbarkeit von Verletzungen der Datensicherheit (Art. 61 Abs. 3 nDSG) als problematisch erachten. Damit steht Art. 2 VE-VDSG in Widerspruch zu einem risikobasierten Ansatz und kann aus folgenden Gründen nicht umgesetzt werden.

- Die in Art. 2 lit. a – k VE-VDSG genannten Schutzziele sind starr und entsprechen nicht den technischen Herausforderungen, welche technologische Entwicklungen und neue Bedrohungen mit sich bringen. Aus den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit können ohne weiteres risikogerechte Massnahmen abgeleitet werden.
- In verschiedenen Bearbeitungszusammenhängen kommt einzelnen, in Art. 2 lit. a – k VE-VDSG genannten Schutzzielen keine Relevanz zu. Vielmehr ist bei der Massnahmendefinition auf die Art und Weise der Bearbeitung abzustellen, um risikogerecht ausgewählte

Schutzziele anzustreben. Die Muss-Formulierung suggeriert demgegenüber eine durchgängige Berücksichtigung bei jeder zu ergreifenden Massnahme.
- Die Formulierung «erreichen» suggeriert, dass Schutzziele zudem bei jeder Massnahme vollständig erfüllt sein müssen. Damit wird der Massstab absoluter Sicherheit bei der Eignungsbeurteilung von Massnahmen angelegt. Somit widerspricht die Formulierung der Einschätzung des Bundesrates, «[e]ine absolute Sicherheit kann und soll nicht verlangt werden» (Erläuterungsbericht, S. 16).
- Die Dokumentationspflicht ist zudem abzulehnen, da diese auch vom Gesetzgeber ausdrücklich abgelehnt wurde.

„müssen" in Artikel 2 ist durch „bezwecken" zu ersetzen, „erreichen" ist durch „anstreben" zu ersetzen. Der Schutzzielkatalog in Artikel 2 lit. a – k ist durch die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit zu ersetzen. Dokumentationspflicht ist zu streichen.

Artikel 3

Die Protokollierungspflicht hat keine gesetzliche Grundlage im nDSG. Die Ausgestaltung der Protokollierungspflicht geht hinsichtlich ihres Gegenstandes, der technischen Modalitäten, der Aufbewahrungsdauer und der engen Zweckbindung zu weit. Deren ansatzweise Umsetzung würde einen organisatorisch-personellen und technischen Aufwand sowie Kosten in ganz unverhältnismässigen Ausmass erfordern. Weiter geht aus den Voten im Parlament sowie aus der finalen Fassung des nDSG hervor, dass am prinzipien- und risikobasierten Regulierungsansatz festgehalten werden soll. Die Ablehnung der Protokollierungspflicht wird im Einzelnen wie folgt begründet.

- Das nDSG sieht keine Protokollierungspflicht vor. Angesichts der massiven finanziellen und technischen Auswirkungen sowie der hier begründeten Strafbewehrung, der Eingriffsintensität in die Wirtschaftsfreiheit sowie der augenscheinlich fehlenden Akzeptanz bei den betroffenen Unternehmen, hätte die Protokollierungspflicht in jedem Fall im Gesetzgebungsprozess behandelt werden müssen.
- Die Protokollierungspflicht ist aus finanzieller Sicht unhaltbar. Neben den Kosten für initiale Implementierungen kämen langfristig Kosten für Lizenzen, Wartung, zusätzliche Personalressourcen sowie die Haltung enormer Datenmengen hinzu. Letzterer Kostenpunkt liesse sich angesichts der Aufbewahrungspflicht von 2 Jahren nicht sachlich begründen. Der Erläuterungspunkt geht also betreffend der Protokollierungspflicht fehl, wenn er von einem blossen «anfänglichen Umsetzungsaufwand» und Auswirkungen «von eher geringer Relevanz» ausgeht (Erläuterungsbericht, S. 13).
- Zu Absatz 1 und 2: Der Wortlaut des VE-VDSG bedient sich mit «automatisierte Bearbeitung von Personendaten» und «hohes Risiko» gemäss einer Datenschutz-Folgenabschätzung unbestimmter Rechtsbegriffe, die zu einer extensiven Protokollierung sämtlicher nicht manueller Bearbeitungstätigkeiten führen würden.
- Zu Absatz 1, 2 und 3: Die Protokollierungsgegenstände als solche sind unverhältnismässig.
- Zu Absatz 2: In Ergänzung zu den vorgenannten Punkten ist bei der Bearbeitung durch Bundesorgane und deren Auftragsbearbeiter festzuhalten, dass die Schweizerische Post AG hier massiv investieren müsste oder die Post Auto AG zum Aufbau eigener Infrastruktur gezwungen wäre, ohne dass dabei die Datensicherheit verbessert würde.
- Zu Absatz 4: Die restriktive Zweckbindung schränkt unnötig ein und bringt keinen Mehrwert für Datenbearbeiter.
- Zu Absatz 4: Die technischen Modalitäten der Protokollierungspflicht sind nicht praktikabel. Einige Bearbeitungszusammenhänge lassen keine systemgetrennte Datenhaltung zu. Bei anderen Bearbeitungszusammenhängen müssten zur systemgetrennten Datenhaltung dezidierte Systeme bereitgestellt werden, um eine hinreichende Betriebsstabilität der Protokolldateien sicherzustellen.
- Zu Absatz 4: Die Aufbewahrungsfrist von 2 Jahren ist ohne allgemeine Dokumentationspflicht, wie sie noch Art. 19 lit. a VE-DSG vorsah, nicht nachvollziehbar und ohne gesetzliche Grundlage. Zudem steht sie in direktem Widerspruch zum Grundsatz der Datenminimierung in zeitlicher Hinsicht.

Artikel 3 ist ersatzlos zu streichen.

Artikel 4

Mit dem Verzeichnis der Bearbeitungstätigkeiten und der Datenschutz-Folgenabschätzung wird die Dokumentation risikobehafteter Datenbearbeitungen hinreichend abgedeckt. Diese Instrumente haben sich unter der DSGVO zur Dokumentation der Bearbeitungstätigkeit bewährt, eine «Swiss Finish» Regelung ist nicht angezeigt, im Gegenteil: Zusätzliche Bearbeitungsverzeichnisse führen ohne erkennbaren, sachlichen Grund zu massivem administrativem Mehraufwand und zu einer Doppelspurigkeit. Im Übrigen findet sich keine gesetzliche Grundlage im nDSG, zumal die generalklauselartige Dokumentationspflicht nach Art. 19 lit. a VE-DSG zugunsten der genannten Instrumente im Gesetzgebungsverfahren entfiel. Der Artikel 4 wird im Einzelnen aus folgenden Gründen abgelehnt.

- Zu Absatz 1: Mit den unbestimmten Rechtsbegriffen «automatisierte Bearbeitungen», «umfangreich [...] bearbeiten» und «Profiling mit hohem Risiko» würde eine Rechtsunsicherheit bezüglich des Dokumentationsumfangs entstehen.
- Aus der Strafbewehrung von Verletzungen der Datensicherheit würde eine überschiessende Dokumentationstätigkeit resultieren, da auch das Bearbeitungsreglement systematisch dem Titel «Datensicherheit» zugeordnet wird.
- Zu Absatz 2: lit. a, b, c und f sind bereits in Art. 12 Abs. 2 nDSG abgedeckt; übrige Angaben werden ohnehin regelmässig als Massnahmen nach Art. 22 Abs. 2 i.V.m. Art. 7 Abs. 1 und 2 nDSG dokumentiert.

Artikel 4 ist ersatzlos zu streichen.

Artikel 5

Ergänzend zu den Ausführungen zu Artikel 4 ist zu bemerken, dass der extensive Katalog zu einer Durchreglementierung der Bearbeitungstätigkeiten von Bundesorganen und deren Auftragsbearbeitern führt. Die Reglementierungspflichten stehen in keinem Verhältnis zu den Risiken der in Art. 1 lit. a – f genannten Tatbestände. Namentlich stellt sich die Frage, weshalb etwa die Reglementierungspflicht bei jeglichem Profiling ohne hohes Risiko notwendig ist. Gemäss Art. 34 Abs. 2 lit. b nDSG ist ohnehin eine gesetzliche Grundlage für Profiling durch Bundesorgane notwendig. Deshalb kann grundsätzlich auf die Risikoabwägungen des Gesetzes- oder Verordnungsgeber abgestützt werden. Entsprechend deren Risikoeinschätzung können punktuelle Reglementierungspflichten in der Sachgesetzgebung festgehalten werden.

Artikel 5 ist ersatzlos zu streichen.

Artikel 6

In Absatz 1 Satz 2 wird eine Sicherstellung vertrags- und gesetzmässiger Bearbeitungen durch Auftragsbearbeiter verlangt. Die Formulierung «sicherstellen» ist zu absolut und auch inhaltlich nicht praktikabel. Wenn, dann kann der Verantwortliche lediglich «dafür Sorge» tragen. Ausserdem resultiert dies in einer kausalen Gewährleistungspflicht des Verantwortlichen, die nicht praktikabel ist. Eine arbeitsteilige Wirtschaft wäre mit einer kausalen Haftung des Verantwortlichen undenkbar und ist der Schweizer Rechtsordnung in dieser Konstellation fremd. Der Verantwortliche trifft in Bezug auf Auftragsbearbeiter nach nDSG eine «*Sorgfaltspflicht* [...] die Rechte der betroffenen Person zu wahren» (Botschaft nDSG, S. 7032). Diese erstreckt sich im Sinne einer verschuldensabhängigen Geschäftsherrenhaftung auf die sorgfältige Auswahl, Instruktion und Überwachung der Auftragsbearbeiter. Damit ist Art. 6 Abs. 1 Satz 2 ohne gesetzliche Grundlage.
Absatz 2 ergibt sich bereits aus der Formulierung von Art. 16 und 17 nDSG.

Artikel 6 Absatz 1 Satz 2 und Absatz 2 sind ersatzlos zu streichen.

Artikel 9
Die namentliche Aufführung von Empfängerstaaten nach Art. 9 Abs. 1 lit. d VE-VDSG sowie internationaler Organisationen nach Art. 9 Abs. 1 lit. e VE-VDSG in vertraglichen Datenschutzklauseln ist ohne gesetzliche Grundlage im nDSG und in der Praxis unverhältnismässig kompliziert. Es genügt, dass analog zu den Standardvertragsklauseln der Europäischen Union die Empfängerinnen und Empfänger nach Art. 9 Abs. 1 lit. g VE-VDSG bezeichnet werden. Im Übrigen haben auch Art. 9 Abs. 1 lit. f und j VE-VDSG keine gesetzliche Grundlage.

Artikel 9 Absatz 1 lit. d, e, f und j sind ersatzlos zu streichen.

Artikel 10
Absatz 1 verlangt, dass der Verantwortliche «sicherstellt», dass Datenschutzklauseln vom Empfänger beachtet werden. Auch hier führt die Vorschrift zu einer Kausalhaftung und ist in der Praxis nicht zu erfüllen. Eine derartig strenge Regelung ist für Unternehmen nicht zumutbar.

Begriff «sicherstellen» in Artikel 10 ist durch «in angemessener Weise für die Einhaltung Sorge zu tragen» zu ersetzen.

Artikel 13
Entgegen des klaren Wortlauts von Art. 19 Abs. 1 nDSG und der Verantwortungsordnung des Datenschutzrechts wird auf dem Verordnungsweg eine Mitverantwortlichkeit des Auftragsbearbeiters für Informationspflichten eingeführt. Es wird in das vertraglich vereinbarte Auftragsverhältnis eingegriffen mit u.a. der Konsequenz, dass der Verantwortliche de facto seine Funktion als Geschäftsherr verliert. Der Rechtssicherheit unzuträglich ist ferner die Erfüllung im telefonischen Setting. Ohne Anlass werden zudem Anforderungen an Piktogramme gestellt. Der Artikel ist praxisfern und ohne gesetzliche Grundlage. Er widerspricht zudem direkt dem Schutzzweck von Art. 19 nDSG. Damit verpasst der VE-VDSG, die Möglichkeit eine praxistaugliche Umsetzung der Informationspflichten vorzuspuren. Konkret ist der Artikel 13 aus folgenden Gründen anzupassen bzw. zu präzisieren.

- Zu Absatz 1 (1): Entgegen des Wortlauts von Art. 19 Abs. 1 nDSG und in Widerspruch zum Prinzip der Verantwortungszurechnung wird eine kumulierte Verantwortlichkeit von Verantwortlichem und Auftragsbearbeiter hinsichtlich der Informationspflichten aufgestellt. Die eigenständige Informationspflicht des Auftragsbearbeiters steht in Widerspruch zu dessen Weisungsbindung. Eine aus der Mitverantwortung des Auftragsbearbeiters erwachsende Vergewisserungspflicht über Herkunft und Empfänger von Personendaten des Verantwortlichen ist im Wirtschaftsverkehr nicht umsetzbar. Dies resultiert in einem beträchtlichen Wettbewerbsnachteil für Schweizer Unternehmen im internationalen Vergleich.
  Die Schweizerische Post ist u.a. auf aktuelle, qualitativ gute Adressdaten angewiesen. Dies stellt die Post für die Schweizer Wirtschaft mit ihren Adressaktualisierungsdienstleistungen sicher. Durch die Mitverantwortlichkeit müsste das Geschäft neu konzipiert werden und viele Partner würden einer entsprechenden Vergewisserungspflicht nicht mit vernünftigen Mitteln nachkommen können. Die Schweizerische Post geht davon aus, dass dadurch die Adressqualität der versendeten Sendungen massiv abnehmen würde und die Post Zusatzkosten aufgrund unzustellbarer Sendungen zu tragen hätte. Dies kann nicht im Sinne des Bundesrates sein.
  Zudem würde die Vervielfachung der Datenschutzerklärungen dem Schutzzweck von Art. 19 nDSG entgegenlaufen. Die resultierende Informationsflut verhindert gerade die einfache Auffindbarkeit und Zugänglichkeit wesentlicher Informationen. Die Informationspflicht von Auftraggebern steht der angestrebten Angemessenheit von Datenschutzinformationen direkt entgegen.
- Zu Absatz 1 (2): Informationssuchende sind auf eindeutige Informationen angewiesen. Die Erfüllung der Informationspflicht über telefonische Beauskunftung würde widersprüchliche und widerrechtliche Situationen schaffen. Es ist im Übrigen Informationssuchenden zumutbar, Datenschutzinformationen im Internet abzurufen. Hinsichtlich der Strafbewehrung sind die daraus resultierenden beweisrechtliche Problematiken unzumutbar.

- Zu Absatz 2: Als ergänzende Informationen dienen Piktogramme in Datenschutzerklärungen in erster Linie dem Verständnis Betroffener. Ohne Not werden zusätzliche Anforderungen an ein betroffenenfreundliches, auf Freiwilligkeit basierendes Instrument gestellt.
- Begrüssenswert wäre die Klarstellung, dass die Informationspflichten in Anlehnung an die Praxis zu Art. 13 DSGVO keine ländergenaue Nennung von Zielstaaten bei Auslandbekanntgaben erfordern. Vielmehr müssen für die betroffenen Personen Länder und die zur Anwendung gelangenden Garantien bei unsicheren Zielstaaten anhand der Angaben bestimmbar sein.

Die Erwähnung des Auftragsbearbeiters ist zu streichen. «Mitteilen» in Abs. 1 ist durch «offenlegen» oder «zugänglich machen» zu ersetzen. Zudem sollte festgehalten werden, dass eine Information über eine Website grundsätzlich genügt. Abs. 2 ist ersatzlos zu streichen.

Artikel 15

In Artikel 15 wird auf Verordnungsebene eine weitere, zusätzliche Informationspflicht eingefügt, die dem Wortlaut von Art. 19 Abs. 1 nDSG widerspricht. Zudem wird eine Vollständigkeit verlangt. Der Artikel ist in der Praxis kaum umsetzbar und ohne gesetzliche Grundlage. Auch diese Pflicht ist im Zusammenhang mit unseren Adressaktualisierungsdienstleistungen kaum mit verhältnismässigem Aufwand umsetzbar. Partner und Kunden der Post müssten künftig Informationen bekanntgeben über die sie aktuell gar nicht verfügen.

Artikel 15 ist ersatzlos zu streichen.

Artikel 16

Artikel 16 verlangt zusätzlich eine aktive Information, sofern Daten berichtigt, gelöscht oder vernichtet wurden. Auch dieser Pflicht fehlt die gesetzliche Grundlage, resp. führt eine Pflicht ein, die im Rahmen der parlamentarischen Beratungen zu Recht gestrichen wurde.

Artikel 16 ist ersatzlos zu streichen.

Artikel 18

Die Bedeutung von «Schriftlichkeit» ist in den Rechtswissenschaften umstritten. Begrüssenswert wäre die Klarstellung, dass eine Nachweisbarkeit durch verschiedene Formen möglich ist. Die «Schriftlichkeit» ist zu eng formuliert.

«schriftlich» durch «nachweisbarer Form» ersetzen.

Artikel 25

Mit der Formulierung «prüft» in Absatz 1 lit. a ist zum einen der Umfang der Prüfung nicht klar. Zum anderen ist fraglich, ob die Prüfung von Bearbeitungen zur Funktion einer Beraterin/eines Beraters gehört. Bereits aus ressourcentechnischen Gründen ist es der Funktion der Datenschutzberatung unmöglich jede beim Verantwortlichen anfallende Bearbeitung zu prüfen. Ferner muss die Datenschutzberaterin/der Datenschutzberater lediglich beratend Einfluss nehmen, damit der Verantwortliche seinen Datenschutzpflichten nachkommt. Die Prüfung der Bearbeitungen muss im Rahmen der Governance mit entsprechenden Aufgaben, Kompetenzen und Verantwortlichkeiten festgelegt werden. Gleiches gilt auch für Absatz 1 lit. b mit der Formulierung «...wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese...» Sinnvollerweise kann sich im Rahmen der Governance eine Konsultationspflicht für die Datenschutzberaterin/den Datenschutzberater ergeben. Die interne «Gewaltenteilung» ist zudem gefährdet. Mit dieser Regelung liegt zudem ein unbegründeter Eingriff in die Privatautonomie des Unternehmens als Verantwortlichen vor. Überdies greift es in die Organisationsfreiheit des Verantwortlichen ein, wie genau die Pflichten gemäss nDSG unter Würdigung der konkreten Verhältnisse im Unternehmen, personell, technisch und organisatorisch am besten erfüllt werden sollen und können. Die Regelung steht auch im Widerspruch mit aufsichtsrechtlichen Vorgaben regulierter Branchen mit grosser Arbeitsteilung.

Artikel 25 Absatz 1 lit. a und b sind ersatzlos zu streichen. Eventualiter ist lit. a zu präzisieren bzw. anzupassen «wird bei Bedarf konsultiert, um Bearbeitungen von Personendaten sowie deren Voraussetzungen auf rechtliche Datenschutzvorschriften zu prüfen».

Im Weiteren möchten wir auf die Stellungnahmen des Vereins Unternehmensdatenschutz, der Swiss Banking sowie des Verbandes öffentlichen Verkehrs (VöV) bei welchen die Schweizerische Post, bzw. PostFinance und PostAuto Mitglied sind, verweisen.

Wir bedanken uns für Ihre Kenntnisnahme und die wohlwollende Prüfung der Eingabe.

Freundliche Grüsse

Die Schweizerische Post AG
Stab CEO GRCS

Gabriele Schmid-Strasser
Datenschutzbeauftragte

Die Schweizerische Post AG
Stab CEO

Matthias Dietrich
Co-Leiter Stab

DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Bundesamt für Justiz
Bundesrain 20
3003 Bern

PER E-MAIL AN jonas.amstutz@bj.admin.ch

13. Oktober 2021

Stellungnahme zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) (Vernehmlassung 2021/26)

Sehr geehrte Damen und Herren

Am 23. Juni 2021 eröffnete der Bundesrat das Vernehmlassungsverfahren zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG). Für die Einladung zum Vernehmlassungsverfahren möchten wir uns bedanken.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

Vorbemerkungen

Ungeachtet der Revision sollten sich die Unternehmen und andere Verantwortliche in der Schweiz grundsätzlich an der europäischen Datenschutz-Grundverordnung (DSGVO) orientieren, da sie mehr Datenschutz garantiert. Verantwortliche, die sich an der DSGVO orientieren, gehen auf Nummer sicher. Das schweizerische Datenschutzrecht hat auch nach der Revision viel Potential, den Datenschutz der betroffenen Personen zu verbessern.

Die Revision des Datenschutzrechts und damit eine gewisse Angleichung an die DSGVO war gleichwohl notwendig. Die Bedeutung eines angepassten und zeitgemässen Datenschutzes ist immens. Ein zeitgemässer Datenschutz bedeutet für betroffene Personen, über ein umfassendes Bild der Datenbearbeitungen zu verfügen, und für die Gesetzgeber:innen die Schaffung von Transparenz und wirksamen Schutzmassnahmen. Die VE-VDSG als Verordnung soll das nDSG konkretisieren und darf nicht darüber hinausgehen. Entgegen einzelnen Ansichten, die bereits heftig und öffentlich geäussert wurden, hält sich die VE-VDSG an den Rahmen des neuen Datenschutzgesetzes (nDSG) und schränkt diesen in gewissen Aspekten sogar ein. Allgemein beinhaltet das VE-VDSG viele schwammige Formulierungen, die den Verantwortlichen unnötige Ermessensspielräume einräumen. Auf diese Schwammigkeit ist zu achten und grundsätzlich zu vermeiden.

Zu den einzelnen Artikeln

Damit ein wirksamer Datenschutz garantiert wird, müssen wirksame Massnahmen getroffen werden. Dazu gehört deren periodische Überprüfung. Die Prüfung der Massnahmen «in angemessenen Abständen», wie in **Artikel 1 Absatz 2 VE-VDSG** festgelegt, ist daher sinnvoll, sollte aber in Bezug auf die Periodizität klargestellt werden («in angemessenen, regelmässigen Abständen»). Nur so kann sichergestellt werden, dass Verantwortliche tatsächlich regelmässig eine Überprüfung vornehmen. Daher ist der zeitliche Faktor relevant. Nach vereinzelten Ansichten sind es die Risikofaktoren, die zu prüfen sind. Diese sind verfehlt. Da sich Massnahmen an Risikofaktoren ausrichten müssen, um wirksam zu sein, sind, wie vorgesehen, in erster Linie die getroffenen Massnahmen zu prüfen. Indirekt werden dadurch auch die Risikofaktoren mitgeprüft.

Die Schutzziele gemäss **Artikel 2 VE-VDSG** müssen nicht nur «angestrebt» werden, wie dies vereinzelt verlangt wird, sondern tatsächlich auch «erreicht» werden, da ansonsten die Schutzschwelle sinkt und gar kein zumindest genügender Datenschutz angestrebt wird. Der Wortlaut ist zutreffend und soll nicht verändert werden. Die Formulierung in Artikel 2 «Soweit angemessen, müssen die Massnahmen … folgende Schutzziele erreichen», ist schwammig. Dies gilt auch für die Ausführungen in den Erläuterungen dazu: «Es ist durchaus vorstellbar, dass nicht jedes Schutzziel in jedem Fall von Relevanz ist. Ist ein Schutzziel in einem Fall nicht von Relevanz, so müssen der Verantwortliche und Auftragsbearbeiter aber in der Lage sein, zu begründen, weshalb dies der Fall ist.». Dadurch erhalten die Verantwortlichen zu grosse

Ermessensspielräume, die befürchten lassen, dass Art. 63 nDSG (strafbare Sorgfaltsverletzung) leer läuft, weil kein Vorsatz mehr nachgewiesen werden kann. Die Formulierung «soweit angemessen» ist daher ersatzlos zu streichen.

Entgegen vereinzelten Ansichten basiert **Artikel 3 VE-VDSG** auf einer genügenden gesetzlichen Grundlage. Ein gewisser Umsetzungsaufwand ist hinzunehmen und der Aufwand richtet sich nach der Stufe der jeweiligen datenschutzrechtlichen Exposition eines Unternehmens oder sonstigen Verantwortlichen (vgl. Erläuterungen). Die Protokollierungspflicht betrifft lediglich Datenbearbeitungen mit hohem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person. Ein Unternehmen, das derartige Datenbearbeitungen vorsieht, ist gehalten, für strengere Datensicherheit zu sorgen.

Ein Profiling ist entgegen vereinzelt anderer Ansicht nie harmlos. Es ist gerechtfertigt und entspricht den risikobasierten Grundsätzen des nDSG, dass bei der Bearbeitung von besonders schützenswerten Personendaten, oder insbesondere bei der Durchführung eines Profiling mit hohem Risiko, höhere Anforderungen an den Datenschutz gestellt werden, wie dies auch in **Artikel 4 VE-VDSG** vorgesehen ist.

Wenn Verantwortliche die Bearbeitung outsourcen, sinkt die Datensicherheit, da mehr Parteien involviert sind, sich die Überprüfungsmöglichkeiten der betroffenen Person verringern und die Transparenz sinkt. **Artikel 6 Absatz 1 VE-VDSG** ist eine essentielle Bestimmung, die zum Schutze einer betroffenen Person ausschlaggebend ist. Wäre es den Verantwortlichen möglich, dieser Verantwortung zu entkommen, hätte dies fatale Folgen für Betroffene.

Neu übernimmt der Bundesrat gemäss Artikel 16 nDSG die Angemessenheitsbeurteilung ausländischer Datenschutzgesetzgebungen und nicht mehr der EDÖB. Der EDÖB soll zwar nach **Artikel 8 Absatz 6 VE-VDSG** vor einer Beschlussfindung noch konsultiert werden, die Entscheidungshoheit bleibt aber beim Bundesrat. Damit dieser Entscheid kein politischer wird und fachkundig bleibt, ist sicherzustellen, dass der EDÖB wie in Absatz 6 festgehalten tatsächlich konsultiert wird und dieser Absatz keine leere Klausel bleibt. Auch hier ist der Transparenzgrundsatz entscheidend, der in Artikel 8 VE-VDSG der Vernehmlassungsvorlage fehlt. Bisher hat der EDÖB die aktuelle Entwicklungen und Anpassungen (siehe z.B. Datenübermittlung in die USA gemäss Swiss-US Privacy Shield) regelmässig auf seiner Website veröffentlicht. Der Bundesrat muss seine Entscheidungen in jedem Fall transparent und für die Öffentlichkeit publik machen, weshalb **Artikel 8 Absatz 3 VE-VDSG** mit folgendem

Satz zu ergänzen ist: «Entscheidungen, Änderungen und Anpassungen sind der Öffentlichkeit begründet, unverzüglich und vollständig zugänglich zu machen».

Artikel 13 Absatz 1 VE-VDSG konkretisiert die Modalitäten der Informationspflicht gemäss Artikel 19 Absatz 1 nDSG und sieht vor, dass die betroffene Person «angemessen» informiert werden soll. In der Botschaft nDSG wird in den Ausführungen zur Informationspflicht bei der Beschaffung von Personendaten (Art. 17) auf die Bedeutung der Transparenz bei der Datenbearbeitung hingewiesen, da sie ein zentrales Ziel der Revision ist. Nur anhand genügender Transparenz können die Rechte der Betroffenen entsprechend gestärkt werden. Der Wortlaut von Artikel 13 Absatz 1 VE-VDSG orientiert sich an Artikel 12 der EU-DSGVO, der die Informationsvermittlung in «präziser, transparenter, verständlicher und leicht zugänglicher Form» vorsieht. Artikel 13 Absatz 1 VE-VDSG beinhaltet das Wort «transparent» entgegen den Ausführungen im Gesetz nicht. Dies kann nur ein Versehen sein. Artikel 13 Absatz 1 VE-VDSG sollte (korrekterweise) analog zur DSGVO ergänzt werden.

Artikel 16 VE-VDSG betrifft die Informationspflicht der Verantwortlichen gegenüber den Empfänger:innen über Berichtigung, Löschung oder Vernichtung sowie die Einschränkungen der Bearbeitung. Dies führt zu Einheitlichkeit bezüglich Datenbearbeitungen, dabei wird aber nicht genügend Transparenz für die betroffene Person geschaffen. Dies entbindet daher die Verantwortlichen nicht von ihrer Informationspflicht gegenüber den betroffenen Personen. Daher muss Artikel 16 VE-VDSGE diesbezüglich und der Klarheit halber mit dem Zusatz «Dies entbindet die Verantwortlichen nicht von ihrer Informationspflicht gegenüber den betroffenen Personen.» ergänzt werden.

Damit sich der EDÖB ein umfassendes Bild im Falle einer Verletzung der Datensicherheit machen kann, sind die in **Artikel 19 Absatz 1 Buchstaben a–g VE-VDSG** vorgesehenen Angaben notwendig. Dies wird auch so in den Erläuterungen zur Vernehmlassungsvorlage betont. Entgegen einzelnen Ansichten geht die Angabe über Zeitpunkt und Dauer nicht über den Rahmen des Gesetzes hinaus, da diese erstens nur gemeldet werden müssen, soweit möglich diese überhaupt vorhanden sind, und zweitens diese Informationen von grundsätzlicher Bedeutung sind, damit das Ausmass der Verletzung abgeschätzt werden kann. Es ist ausserdem für alle beteiligten Parteien wichtig, dass die Verletzung dokumentiert wird, wie dies in Artikel 19 Absatz 5 VE-VDSG vorgesehen ist. Die Aufbewahrungsdauer von drei Jahren ist vorliegend nicht

die einzige dreijährige Frist wie vereinzelt behauptet wird, auch das Auskunftsrecht nach Artikel 20 Absatz 5 VE-VDSG sieht eine dreijährige Aufbewahrungsfrist der Aufzeichnungen im Falle einer Verweigerung, Einschränkung oder Aufschiebung der Auskunft vor. Artikel 19 VE-VDSG beinhaltet die Pflicht eine Verletzung der Datensicherheit und deren Umstände aufzuzeichnen. Artikel 20 VE-VDSG legt fest, dass die Gründe für eine Auskunftsverweigerung, -einschränkung oder -aufschiebung zu dokumentieren sind. Beide Artikel sind wichtig für eine betroffene Person, da sie ihr ermöglichen, sich rechtlich zur Wehr setzen zu können. Daher macht eine Aufbewahrungsfrist von drei Jahren in beiden Fällen Sinn.

Artikel 20 Absatz 1 VE-VDSG: Artikel 25 nDSG nennt ausdrücklich nur «Auskunft», es steht nicht, ob die Auskunft mündlich oder schriftlich gestellt werden muss. Dass die Auskunft mündlich gestellt werden kann, ist selbstverständlich. Die Form des Begehrens kann aber nicht vom Willen der Verantwortlichen abhängig gemacht werden, dabei würde die Tür zur Willkür geöffnet. Demnach geht Artikel 20 Absatz 1 VE-VDSG zu weit, wenn die Zulässigkeit des mündlichen Begehrens von den Verantwortlichen abhängig gemacht wird. Das Auskunftsrecht ist ein wesentlicher Grundsatz des Datenschutzes. In den Erläuterungen wird zur Begründung auf den Kommentar des Bundesamtes für Justiz zur Vollzugsverordnung vom 14. Juni 1993 (Stand am 1. Januar 2008) zum Bundesgesetz über den Datenschutz (VDSG, RS 235.11) verwiesen. Diese Ausführungen sind nicht aktuell und orientieren sich noch an anderen Zeiten. Um die Rechte der betroffenen Personen zu stärken, ist es daher wichtig, sich an aktuellen Gegebenheiten zu orientieren. Daher sind mündliche Auskunftsbegehren nicht vom Willen der Verantwortlichen abhängig zu machen.

Die Dokumentation der Auskunftsverweigerung ist Ausfluss des Transparenzprinzips und stärkt die Rechte der betroffenen Personen. Diese ist daher unbedingt beizubehalten. Es ist gemäss Artikel 8 Absatz 3 nDSG Aufgabe des Bundesrates, Bestimmungen über die Mindestanforderungen an die Datensicherheit zu erlassen. Artikel 20 VE-VDSG geht in diesem Sinne, entgegen vereinzelter Ansicht, nicht weiter als das Gesetz und verfügt über eine gesetzliche Grundlage.

Artikel **22 Absatz 1 VE-VDSG** trägt ebenfalls zur Stärkung der Rechte der betroffenen Personen bei. Die Frist von 30 Tagen ist klar. Entgegen einzelner Ansichten ist die Frist nicht von einer Bedingung abhängig zu machen, denn dies würde den Verantwortlichen einen zu grossen Ermessensspielraum einräumen, der die Rechte der betroffenen Personen erheblich einschränken würde. Artikel 22 Absatz 2 VE-VDSG

relativiert Absatz 1 und birgt die Gefahr, dass ein Auskunftsbegehren unbegrenzt in die Länge aufgeschoben werden könnte. Dies gefährdet die Rechte der betroffenen Personen. Die Frist ist auf eine maximale Dauer zu begrenzen.

Artikel 23 VE-VDSG regelt die Ausnahmen von der Kostenlosigkeit und konkretisiert Artikel 25 Absatz 6 nDSG. Eine Ausnahmeregelung zur Kostenlosigkeit besteht bereits heute und wird in der Praxis oft missbraucht, um den Spielraum der Abwehrmöglichkeiten von Datenauskunftsbegehren auszuweiten. Diesen Spielraum darf zum Schutz der betroffenen Personen nicht bestehen bleiben (oder durch eine Erhöhung des Betrags sogar ausgeweitet werden). Das Auskunftsrecht darf nicht durch diese Abschreckungswirkung ausgehöhlt werden. Zu betonen ist: Gemäss dem Grundsatz «Privacy by Design» sind die Verantwortlichen verpflichtet, ein System zu führen, das einen einfachen Zugang zu den bearbeiteten Daten ermöglicht. Falls die Verantwortlichen aufgrund eigenem Unvermögen einem «unverhältnismässigen» Aufwand aufgrund eines Auskunftsgesuches gegenüberstehen (was bei vielen Verantwortlichen zu befürchten ist), ist dies in keinerlei Weise Grund zur Auferlegung von Kosten auf betroffene Personen. Deshalb ist Artikel 23 VE-VDSG dahingehend zu ändern, dass die Auskunftserteilung immer kostenlos ist, unabhängig des Aufwands und im seltenen Falle eines klar rechtsmissbräuchlichen Auskunftsbegehrens, dieses abgewiesen würde. Verantwortliche, die häufig oder komplex Auskunft erteilen müssen, erhalten einen Anreiz, die Auskunftserteilung zu automatisieren.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen ist damit keine Zustimmung durch die Digitale Gesellschaft zu solchen Regelungen verbunden.

Mit freundlichen Grüssen

Erik Schönenberger
Geschäftsleiter

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin
Karin Keller-Sutter
Bundeshaus West, 3003 Bern

Einreichung per Mail an: jonas.amstutz@bj.admin.ch

Bern, 13. Oktober 2021

Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Stellungnahme von digitalswitzerland

Sehr geehrter Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zur «Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz» (VDSG) äussern zu können. Diese Gelegenheit nimmt der Verein digitalswitzerland gerne wahr.

1 Betroffenheit digitalswitzerland

digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 240 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartnerin in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.

2 Es braucht eine ausführliche Überarbeitung des Entwurfs

In einer zunehmend digitalisierten Wirtschaft ist es von zentraler Bedeutung, dass die Datenschutzgesetzgebung eine Balance zwischen dem angemessenen Schutz von Daten und der wirtschaftlichen und wissenschaftlichen Nutzung von Daten findet. Die Schweizer Digitalwirtschaft setzt sich für einen modernen und zweckmässigen Datenschutz ein, der die Innovationskraft des Standorts Schweiz nicht behindert. Ein administrativ tragbares Vorgehen im Rahmen der internationalen Entwicklungen ist dabei zentral.

Mit dem *revidierten Datenschutzgesetz (resDSG)* wurde im Herbst 2020 ein modernes Gesetz geschaffen, welches das Schutzniveau der *Datenschutz-Grundverordnung der EU (DSGVO)* übernimmt, die Anliegen der Politik und Wirtschaft angemessen berücksichtigt und zahlreiche Verbesserungen gegenüber dem bisherigen Datenschutzgesetz (DSG) beinhaltet. Gerade durch seine Angleichung an die DSGVO wird das neue resDSG für die Schweizer Unternehmen gut umsetzbar. Leider ist man bei der Erarbeitung der Verordnung jedoch von diesem wichtigen Prinzip abgekommen. Eine grosse Menge an Sonderregeln haben als «Swiss Finish» ihren Weg in den *Entwurf zur Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)* gefunden. Die Abweichungen sind weder notwendig noch zweckmässig und führen zu einem enormen Mehraufwand für Schweizer Organisationen.

Zudem wurde der politische Prozess bei der Erarbeitung des E-VDSG nicht ausreichend berücksichtigt. So wurden Regelungen, welche im politischen Prozess um die DSG-Revision im Parlament abgelehnt worden waren, in der E-VDSG wiederbelebt (Art. 16 E-VDSG). Zwar ist der Bundesrat berechtigt, Gesetze durch Verordnungen näher auszuführen (Art. 182 Abs. 2 BV); dabei darf er aber nur «Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher ausführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beitragen» (BGE 141 II 169). Mehrere Regelungen im E-VDSG haben diesen Rahmen klar gesprengt, indem sie einen mit den Bestimmungen im revDSG vergleichbaren Regelungsgehalt aufweisen (z.B. Art. 4, Art. 15 und Art. 16). Es ist nicht Aufgabe der Verwaltung, ein parlamentarisches Gesetz nach Abschluss des Gesetzgebungsprozesses auf dem Verordnungsweg zu verschärfen.

Zusammengefasst: Der vorliegende E-VDSG verschärft wesentliche Punkte des Gesetzes, ist inhaltlich nicht ausreichend präzise und unnötig restriktiv. Statt das revDSG im Sinne von Ausführungsvorschriften zu konkretisieren, sieht die Verordnung eine Reihe von bürokratischen Zusatzvorschriften vor, die keine Grundlage im Gesetz finden.

Eine vernünftige Umsetzung der Datenschutzgesetzgebung ist für die digitale Wirtschaft und damit für die Zukunftsfähigkeit und Innovationskraft des Wirtschaftsstandorts Schweiz entscheidend. Der Bund fördert Digitalisierung umfassend und auf allen Stufen. Folgerichtig sollte er das auch beim Thema Datenschutz tun.

Weiter ist der verschärfte E-VDSG mit Blick auf die von KMU geprägte Struktur der schweizerischen Wirtschaft gravierend. Viele der Vorschriften lassen sich entweder gar nicht (Art. 2 E-VDSG) oder nur mit unverhältnismässigem Aufwand umsetzen. Diese Aussicht ist besonders besorgniserregend, weil viele der Pflichten mit strafrechtlichen Sanktionen (Art. 60ff. revDSG) bedroht sind.

Konsequenz: Aufgrund der oben geschilderten Ausgangslage wird der vorliegende Entwurf von digitalswitzerland abgelehnt. Er stellt keine Grundlage für einen zweckmässigen, zukunftsgerichteten Datenschutz dar.

3 Forderungen und Hauptanliegen

Der E-VDSG und der Erläuterungsbericht müssen unter Respektierung der Kohärenz zum revDSG ausführlich überarbeitet werden. Swiss Finishs und unnötigen Restriktionen sind zu vermeiden. Die Überarbeitung muss unter Einsetzung der notwendigen Ressourcen zeitnah dahingehend erfolgen, dass die Äquivalenz aufrechterhalten werden kann.

Die wichtigsten Kritikpunkte und Forderungen für die Überarbeitung sind aus Sicht von digitalswitzerland folgende:

1) Artikel und Prinzipien, welche im politischen Prozess abgelehnt und aus dem Entwurf zum revDSG gestrichen wurden, sollen nicht durch die VDSG wieder eingeführt werden. So z.B. Art. 16, der eine Informationspflicht einführen möchte, von der man sich im Vernehmlassungsprozess zum revDSG verabschiedet hatte.
2) Zahlreiche Swiss Finishs führen zu zwei Standards für Schweizer Organisationen. Die folgenden Artikel sind dabei besonders gravierend und müssen entweder gestrichen oder dahingehend geändert werden, dass sie keine zusätzlichen, über die DSGVO hinausgehenden, Pflichten beinhalten:
    a. Art. 4 Abs. 1 E-VDSG
    b. Art. 13 Abs. 1 E-VDSG
    c. Art. 15 E-VDSG
    d. Art. 19 E-VDSG
3) Widersprüche wie in Art. 13 E-VDSG müssen unbedingt behoben werden. Der Artikel kreiert eine Inkonsistenz in Bezug auf Art. 19 revDSG, Art. 13f. DSGVO und auch zum bisherigen Gesetz (Art. 14 DSG).
4) Weitere zentrale Änderungsvorschläge beziehen sich auf folgende Artikel:
    a. Art. 3 E-VDSG
    b. Art. 8 E-VDSG
    c. Art. 16 E-VDSG

4 Anpassungsvorschläge und Begründungen im Detail

Im Anhang ab Seite 4 werden ausformulierte Anpassungsvorschläge aufgeführt. Diese sind in Abstimmung mit dem Wirtschaftsdachverband economiesuisse entstanden.

Wir danken Ihnen für die Aufmerksamkeit, die Sie unseren Anliegen entgegenbringen und stehen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Nicolas Bürer
Managing Director digitalswitzerland

Andreas W. Kaelin
Deputy Managing Director digitalswitzerland

Für weitere Auskünfte:
Andreas W. Kaelin, digitalswitzerland | Geschäftsstelle Bern
Tel. +41 31 311 62 45 │ andreas@digitalswitzerland.com

5 Anhang: Anpassungsvorschläge im Detail

Anliegen im Falle einer Weiterführung des bisherigen Entwurfs

Kapitel 1: Allgemeine Bestimmungen

Artikel 1 (Grundsätze)

Antrag:

1. Sachlogische Anpassung beim Begriff «Risiko».
2. Berücksichtigung des Implementierungsaufwands statt der -kosten als Kriterium aufnehmen.
3. Anerkennung eines Umsetzungsermessens des Verantwortlichen.

Begründung:

1. Ein Risiko ergibt sich sachlogisch vorab aus einer potenziellen Verletzung der Datensicherheit für die betroffene Person. Für den Fall des Vorliegens einer solchen potenziellen Verletzung stellt sich nachgelagert die Frage nach der Eintrittswahrscheinlichkeit. Dabei sind die Anforderungen an die Datensicherheit höher, je grösser die Eintrittswahrscheinlichkeit ist. Ohne potenzielle Datensicherheitsverletzung stellt sich umgekehrt die Frage nach der Eintrittswahrscheinlichkeit gar nicht. Die Formulierung in Art. 1 Abs. 1 lit. b E-VDSG ist verwirrend, weil sie diese sachlogisch zwingende Reihenfolge nicht beachtet. Die Formulierung in lit. b ist deshalb richtigerweise umzudrehen.
2. Die Aufführung der Implementierungskosten als Kriterium zur Beurteilung der Angemessenheit von technischen oder organisatorischen Massnahmen (sog. TOM) zur Gewährleistung der Datensicherheit ist unseres Erachtens nicht ausreichend. Neben eigentlichen Implementierungskosten fallen typischerweise auch weitere Aufwendungen an, welche zu berücksichtigen sind – so etwa personelle, zeitliche und organisatorische Aufwendungen. Innerhalb einer Auswahl gleichwertiger angemessener Massnahmen darf der Verantwortliche die kostengünstigere auswählen. Dies ist selbstverständlich, da es sich bereits aus dem allgemeinen Verhältnismässigkeitsprinzip ergibt, wird sinnvollerweise aber dennoch erwähnt.
   Zudem sollte nicht allein auf die Implementierungskosten, sondern generell auf den Implementierungsaufwand, der etwa aus personellen, zeitlichen und organisatorischen Aufwendungen besteht, abgestellt werden.
3. Ob, wann und wie eine Überprüfung der TOM stattfinden soll, muss durch den Verantwortlichen bzw. den Auftragsbearbeitenden selbst entschieden werden. Nur er/sie ist in der Lage, den Besonderheiten des Einzelfalls hinreichend Rechnung zu tragen. Ist die Gefährdung der Rechte von Betroffenen grösser, so ist der zeitliche Abstand bis zur nächsten Prüfung sachlogisch kürzer. Die einseitige Fokussierung auf den zeitlichen Abstand einer Prüfung und die zwingende Verknüpfung einer Prüfpflicht ist somit nicht sachgerecht, unnötig einengend und steht im Widerspruch zum risikobasierten Ansatz. Der Begriff «angemessene Abstände» ist durch «angemessene Weise» zu ersetzen.

Formulierungsvorschlag:
1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:
a. […];
b. die verbleibenden ~~Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren~~ potenziellen Auswirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit
c. […];
d. Implementierungs~~kosten~~aufwand.
2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessener~~n~~ ~~Abständen~~ Weise zu überprüfen.

Artikel 2 (Schutzziele)

Antrag:
Der Verordnungstext bringt zu wenig klar zum Ausdruck, dass sich die Notwendigkeit der in Art. 2 E-VDSG aufgeführten Schutzziele nach den in Art. 1 E-VDSG vorgeschriebenen Grundsätzen richtet.

Begründung:
Die in Art. 2 Abs. 2 E-VDSG aufgeführten Schutzziele sind veraltet, zu absolut und zu detailliert geregelt. Entsprechend ihrer abstrakten Formulierung erwecken die Schutzziele zudem fälschlicherweise den Eindruck, dass es sich um absolut zu erreichende Anforderungen handelt. Insofern werden statt Minimalanforderungen fälschlicherweise Maximalanforderungen formuliert.

Im Kern muss es im - hier zu regelnden - Bereich der Datensicherheit um die Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit gehen. Eine generelle Dokumentationspflicht ist schon deshalb abzulehnen, weil diese so auch vom Gesetzgeber ausdrücklich abgelehnt worden ist.

Selbst die tatsächlich aufzuführenden Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit haben nur beispielhaften Charakter. Sie müssen namentlich dann nicht umgesetzt werden, wenn die Analyse nach Art. 1 E-VDSG dies nicht gebietet. Die Formulierung in der Verordnung sollte dies deutlich zum Ausdruck bringen. Damit sollen nicht zuletzt auch KMU vor unnötigem administrativem Aufwand bewahrt werden. Die vorgeschlagenen Formulierungen bringen zum Ausdruck, dass die Aufzählung in Art. 2 E-VDSG weder vollständig noch verpflichtend ist. Umgesetzt werden muss nur das, was nach Art. 1 E-VDSG zur Gewährleistung einer angemessenen Datensicherheit notwendig ist. Um dieses Ziel zu erreichen, können jedoch auch Massnahmen zur Anwendung kommen, die in Art. 2 E-VDSG nicht erwähnt sind. Mit den von uns beantragten Anpassungen ist die Liste auch konform mit den Anforderungen von Art. 32 EU-DSGVO. Ohne entsprechende Anpassungen läge demgegenüber ein kontraproduktiver Swiss Finish vor, welcher wegen unnötigen Zusatzaufwendungen und Zusatzrisiken auch die EU-Äquivalenz gefährden würde.

Formulierungsvorschlag
~~Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen~~ Basierend auf den Grundsätzen nach Art. 1 ist insbesondere zu beurteilen, welche der nachfolgenden Schutzziele für Systeme und Dienste in Zusammenhang mit der Bearbeitung von Personendaten in Anwendung des risikobasierten Ansatzes im konkreten Fall anwendbar sind:
a. Vertraulichkeit
b. Integrität
c. Verfügbarkeit
d. Belastbarkeit

Artikel 3 (Protokollierung)

Antrag:
Ersatzlos streichen.

Begründung:
Diese Bestimmung ist in mehrfacher Hinsicht problematisch. Das Parlament hat trotz detaillierter Formulierung der Anforderungen an die Datenschutzfolgenabschätzungen in Art. 22 revDSG bewusst auf eine Protokollierungspflicht verzichtet. Darüber hinaus ergibt sich aus zahlreichen Voten im Parlament ebenso wie aus der finalen Fassung des revDSG mit aller wünschbaren Deutlichkeit, dass das Parlament – auch ausserhalb des Datenschutzrechts – am bewährten prinzipien- und risikobasierten Regulierungsansatz festhalten wollte und –

nicht zuletzt, um unnötigen Aufwand für die zahlreichen KMU zu verhindern – namentlich auf unnötige Formvorschriften verzichten wollte. Dazu gehören neben strikt formulierten Dokumentations- und Protokollierungspflichten u.a. auch strikte Aufbewahrungsfristen (deren Dauer über die E-VDSG verteilt zudem eher zufällig mal kürzer, mal länger geregelt werden). Die Festlegung der geeigneten organisatorischen und technischen Massnahmen (TOM) zur Umsetzung von Pflichten gemäss revDSG muss in Anwendung des im revDSG bewusst gewählten prinzipien- und risikobasierten Ansatzes jedem Verantwortlichen bzw. Auftragsbearbeiter nach vernünftigem Ermessen obliegen, namentlich entsprechend den Kriterien Grösse, Struktur, Komplexität, Risiken und Geschäftsmodell (vgl. schon oben Ziff. A. 1-7). Nach alledem widerspricht die in Art. 3 E-VDSG vorgeschlagene Protokollierungspflicht dem klaren gesetzgeberischen Willen, hat somit keine gesetzliche Grundlage und wäre überdies auch in seinen Wirkungen kontraproduktiv, würden doch in Anwendung dieser Pflicht umfassende Protokolle bzw. Logs über praktisch sämtliche Personendatenflüsse eines Verantwortlichen erstellt. Eine solche Pflicht auf Stufe E-VDSG wäre eine klare Verletzung des im revDSG verankerten Verhältnismässigkeitsprinzips (vgl. namentlich Art. 6 Abs. 2 u. 3 revDSG), mithin dem wohl wichtigsten Grundprinzip für ein funktionierendes Datenschutzsystem. In Anwendung von Art. 3 E-VDSG würden denn auch statt Datenschutzprobleme gelöst, auf widersinnige Weise neue geschaffen. Zuletzt müsste auch der Auftragsbearbeiter protokollieren, der aber u.U. gar nicht weiss, ob eine Folgeabschätzung durchgeführt wurde und was ihr Ergebnis war.

Nach alledem ist Art. 3 E-VDSG konsequenterweise **ersatzlos zu streichen**.

Eventualiter:
Will man wider Erwarten nicht so weit gehen, müsste zumindest die Anforderung «Protokollierung» durch «angemessene Dokumentation» ersetzt werden, sowie in Abs. 4 «Protokolle mindestens 2 Jahre aufzubewahren» durch: «Die Aufbewahrungsfrist muss, sofern eine solche gesetzlich festgelegt ist, abhängig von Dauer und Datenbearbeitung und generell angemessen sein».

Artikel 4 (Bearbeitungsreglement von privaten Personen)

Antrag:
Ersatzlos streichen.

Begründung:
Die Regelung wurde im Wesentlichen aus Art. 11 der geltenden VDSG übernommen. Schon jene Bestimmung blieb aber insofern «toter Buchstabe», als es ein solches «Bearbeitungsreglement» in dieser Form in der operativen Praxis von Unternehmen nicht gibt. Vielmehr werden die zahlreichen notwendigen Regelungen gemäss bewährter Usanz in einem ganzen Paket von sich gegenseitig ergänzenden Weisungen samt dazugehörigen Prozessen und Listen mit Aufgaben, Kompetenzträgern und Verantwortlichkeiten abgebildet. Diese sind sehr viel wirkungsvoller als ein starres Reglement. Das in der E-VDSG vorgesehene Bearbeitungsreglement kann die immer komplexeren Datenbearbeitungen in der Praxis nicht mehr sinnvoll abbilden. Diese Aufgabe übernimmt zu Recht das neu zu führende Verzeichnis der Bearbeitungstätigkeiten (Art. 12 revDSG).

Umso unverständlicher ist, dass die Regelung von Art. 4 E-VDSG weitgehend deckungsgleich mit den Anforderungen an das gemäss Art. 12 revDSG zu erstellenden Verzeichnis der Bearbeitungstätigkeiten ist, was unnötigerweise Rechtsunsicherheit und unnötigen Doppelaufwand produziert. Das revDSG sieht in Art. 12 bereits vor, dass die Datenverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten führen müssen. Dieses muss ähnliche Informationen enthalten wie das Bearbeitungsreglement. Mit der Einführung des Verzeichnisses macht ein zusätzliches Bearbeitungsreglement keinen Sinn, zumal dieses weitgehend die gleichen Informationen enthält.

Die Aufgreifkriterien gemäss Art. 4 Abs. 1 E-VDSG sind keineswegs klar abgrenzbar. Im Bereich Profiling besteht unter Würdigung sämtlicher Kriterien ein gewisses Ermessen, wann die Grenze zu «hohem Risiko» erreicht ist. Die gesetzliche Regelung (vgl. Art. 5 lit. f und g revDSG) gibt hierzu auch keine klaren Vorgaben, weil nur technische Beschreibungen ohne echte Abgrenzungskriterien festgelegt wurden. Namentlich wiederholt die Regelung für Profiling mit hohem Risiko (Art. 5 lit. g revDSG) im Kern einen technischen Beschrieb, welcher auf jedes Profiling zutrifft und lässt offen, wann die Grenze zu einem «hohen Risiko» erreicht ist. Kritisch ist auch das Aufgreifkriterium «Bearbeitung umfangreicher besonders schützenswerter Personendaten» gemäss Art. 4 Abs. 2 Abs. 1 lit. b E-VDSG. Dies dürfte bei HR-Daten rasch der Fall sein, auch bei den KMU. Die offene Formulierung «umfangreich» ist deshalb als Aufgreifkriterium nicht geeignet. Nach alledem müssten sorgfältige Verantwortliche im Zweifelsfall einen Grossteil ihrer Datenbearbeitungen den Regeln von Art. 4 E-VDSG unterstellen. Gemäss Systematik von Art. 4 Abs. 1 E-VDSG ist dies aber gar nicht beabsichtigt, soll doch Art. 4 E-VDSG nur auf Ausnahmen von der Regel anwendbar sein. Diese misslungene Regelung ist ein eigenständiger Grund für die ersatzlose Streichung von Art. 4 E-VDSG.

Auch hat ein Bearbeitungsreglement mit der Datensicherheit im eigentlichen Sinne, die Art. 8 Abs. 3 revDSG regelt, nicht zu tun. Es fehlt daher die gesetzliche Grundlage für eine Pflicht, ein Bearbeitungsreglement zu führen.

Art. 4 E-VDSG generiert somit statt Klärung bloss Verwirrung und unnötige Abgrenzungsprobleme. Zwei weitgehend deckungsgleiche Regelungen zu erlassen, ist gänzlich sinnlos. Dies umso mehr, als die meisten Schweizer Unternehmen überdies auch grenzüberschreitende Geschäfte betreiben und deshalb entsprechende Verzeichnisse nicht nur nach dem revDSG, sondern überdies auch nach der EU-DSGVO erarbeiten müssen.

Demzufolge ist Art. 4 E-VDSG **ersatzlos zu streichen**.

Artikel 6 (Modalitäten)

Antrag:

1. Klarstellung im Erläuterungsbericht, dass die VDSG – anders als die DSGVO – keinen Mindestinhalt an den Auftragsdatenverarbeitungsvertrags (ADV) vorschreibt.
2. Streichung von Abs. 1
3. Streichung von Abs. 2

Begründung:

1. Es ist unklar, was die Ausführungen auf S. 24 der Erläuterungen zu den Anforderungen an den Inhalt des ADV gemäss Art. 22 Abs. 3 DSGVO bezwecken, zumal diese in Art. 6 E-VDSG nicht vorgesehen sind. Diese Ausführungen suggerieren, dass der ADV gemäss Art. 6 VDSG den inhaltlichen Anforderungen der DSGVO genügen müsse. Hierfür findet sich indes keine gesetzliche Grundlage. Auch die E-VDSG enthält keine inhaltlichen Vorgaben.
2. Absatz 1 wiederholt zuerst eine Banalität und ist gleichzeitig ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall eingeschränkt ist, auch dann, wenn ihm nichts vorgeworfen werden kann. Dem sollte nicht so sein. Es ist ohnehin nicht klar, was mit «für den Datenschutz verantwortlich» gemeint ist. Strafrechtliche Verantwortlichkeit kann es nicht sein und aufsichtsrechtliche Verantwortlichkeit setzt ebenfalls Kontrollmöglichkeiten voraus. Wird die Verantwortlichkeit schliesslich als zivilrechtliche Haftung verstanden, dann wird mit dieser Regelung eine vom Gesetzgeber nicht vorgesehene Kausalhaftung eingeführt. Hierfür fehlt eine gesetzliche Grundlage. Dies würde auch

über Art. 82 Abs. 3 DSGVO hinausgehen. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR. Zudem ist die Formulierung «sicherstellen» inhaltlich falsch. Der Verantwortliche kann nur «dafür Sorge tragen».
Auch dem zweiten Satz fehlt eine gesetzliche Grundlage. Nach Art. 9 Abs. 1 lit. a revDSG hat der Verantwortliche dafür zu sorgen, dass die Daten so bearbeitet werden, wie er es selbst darf. Nach Satz 2 hat er jedoch auch für die Durchsetzung seines eigenen Vertrags zu sorgen, selbst wenn dieser strenger sein sollte als das Gesetz. Macht er also einen zu strengen Vertrag, erlaubt aber seinem Auftragsbearbeiter eine Bearbeitung, die dem noch Gesetz entspricht, ist diese Vorschrift bereits verletzt. Die Regel verwirrt also mehr als sie nutzt. Schon nach Art. 9 Abs. 1 lit. a revDSG hat der Verantwortliche dafür zu sorgen, dass das DSG eingehalten wird. Das sollte genug Schutz bieten, sodass die Regelung hier obsolet wird.

3. Der Sinn und Zweck der Regelung von Abs. 2 erschliesst sich nicht, da der Regelungsgehalt bereits durch die Art. 16 und 17 revDSG (Bekanntgabe von Personendaten ins Ausland) abgedeckt ist. Gemäss Erläuterungsbericht entspricht der neue Art. 6 Abs. 2 E-VDSG dem geltenden Art. 22 Abs. 3 VDSG. Dabei handelt es sich aber um eine Bestimmung für Bundesorgane, während Art. 6 Abs. 2 E-VDSG sowohl für Datenbearbeitungen Privater als auch für solche von Bundesorganen gelten soll. Aus dem Erläuterungsbericht geht nicht hervor, warum diese Bestimmung nun auch für Private gelten soll. Offen bleibt auch, weshalb es die Regelung überhaupt braucht bzw. auf welche Rechtsgrundlage sie sich stützt.
   Die Regelung würde nur dort halbwegs Sinn machen, wo ein Schweizer Verantwortlicher einen ausländischen Auftragsbearbeiter einsetzt, um Daten zu bearbeiten, ohne dass es zu einer Bekanntgabe aus der Schweiz kommt und somit Art. 16 revDSG nicht greift. Systematisch wäre aber auch dieser Fall in Art. 16 revDSG zu regeln und nicht in der VDSG. Zudem ist diese Konstellation ein absoluter Sonderfall. Eine eigene Regelung in der E-VDSG rechtfechtfertigt sich somit nicht. Die Regelung ergibt sich im Übrigen ohnehin bereits aus Art. 9 Abs. 1 lit. a revDSG, und zwar systematisch korrekt, während sie hier systematisch falsch angelegt ist: Im Falle einer Auftragsbearbeitung geht es um die Sicherstellung eines gleichwertigen Datenschutzes, da der Auftragsbearbeiter die Daten gar nicht in eigener Regie bearbeiten darf. Vielmehr geht es darum sicherzustellen, dass die Daten nur so bearbeitet werden, wie der Verantwortliche dies darf – und so steht es schon in Art. 9 Abs. 1 lit. a revDSG.

Aufgrund obiger Ausführungen sind Art. 6 Abs. 1 sowie Abs. 2 E-VDSG **ersatzlos zu streichen**.

Artikel 8 (Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs)

Antrag:
Sowohl in Abs. 1 als auch in Abs. 3 und 6 braucht es eine Anpassung, um klarzustellen, dass sich die Regelung nur an den Bundesrat richtet.

Begründung:
Nach Art. 16 Abs. 1 revDSG legt nunmehr der Bundesrat fest, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten.

Der Wortlaut von Art. 8 Abs. 1 und 6 E-VDSG kann dahingehend missverstanden werden, dass die verantwortliche Stelle – und nicht der Bundesrat – die Angemessenheit des Datenschutzes in einem Empfängerstaat feststellen muss. Somit muss klargestellt werden:

- dass sich dieser Artikel nur an den Bundesrat (BR) richtet;
- dass der BR einzige kompetente Stelle wird, welche eine solche Positiv-Liste erlassen kann – der EDÖB wird vom BR konsultiert, kann jedoch keine eigene Liste herausgeben. Die Aufgabe des EDÖB liegt neu

lediglich darin, Empfehlungen/Assessmentvorgaben für den Datentransfer in Länder zu formulieren, die nicht auf der Positiv-Liste sind;
- dass die Positiv-Liste des BR verbindlich ist.

Formulierungsvorschlag:
1 Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~ muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen~~t werden~~:
[…]
6 Der Bundesrat konsultiert den EDÖB ~~wird~~ vor jedem Entscheid über die Angemessenheit des Datenschutzes ~~konsultiert~~.

Implikationen als Folge der Rechtsprechung des Europäischen Gerichtshofs (EuGH) in der Rechtssache Schrems II sowie des Positionspapiers und der Handlungsanleitung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in gleicher Sache (Art. 8 Abs. 1 Satz 2 E-VDSG und Abs. 7 E-VDSG).

Wie bereits erwähnt, legt nunmehr der Bundesrat fest, welche Staaten oder internationale Organe einen angemessenen Datenschutz gewährleisten. Gemäss dem erläuternden Bericht des Bundesamtes für Justiz soll daher die Verordnung neu die Kriterien regeln, welche der Bundesrat bei seinem Entscheid berücksichtigt. In Anhang 1 sind tabellarisch diejenigen Staaten und internationalen Organe aufgeführt, welche über ein angemessenes Datenschutzniveau verfügen.

Der Bundesrat erstellt die Liste der Länder mit angemessenem Datenschutz nach bestem Wissen und Gewissen. Die Verantwortlichen dürfen sich auf diese Liste im Prinzip verlassen und müssen nicht per se eigene Abklärungen vornehmen, welche die Einschätzung des Bundesrates bestätigen. Die Liste geniesst aber keinen öffentlichen Glauben (anders als z.B. das Grundbuch). Die Verantwortlichen dürfen sich deshalb nur so lange auf Gutgläubigkeit berufen und sich auf die Liste verlassen, wie ihnen aus eigener Erfahrung nichts Gegenteiliges bekannt ist. Ohne dahingehenden eigenständigen Verdachtsanlass selbst Abklärungen über die Richtigkeit der Liste vornehmen muss der Verantwortliche aber nicht (vgl. schon BJ-Erläuterungen zum DSG vom 24. März 2006, S. 8, Antwort zu Frage 49).

Am 18. Juni 2021 hat der EDÖB eine Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug veröffentlicht. Soweit danach ein Land auf der Staatenliste (des EDÖB und künftig des Bundesrates) fehlt oder mit einem ungenügenden Schutzniveau ausgewiesen ist, muss der Datenexporteur prüfen, ob kumulativ folgende vier Garantien eingehalten werden:

- klare Rechtsgrundlage betreffend Zwecke sowie Verfahren und materiellrechtliche Voraussetzungen des behördlichen Datenzugriffs und Befugnisse der Behörden;
- Verhältnismässigkeit der behördlichen Befugnisse und Massnahmen;
- wirksame, gesetzlich verankerte Rechtsbehelfe für die Durchsetzung von Rechten von Betroffenen in der Schweiz;
- Rechtsweggarantie und Zugang zu einem unabhängigen und unparteiischen Gericht.

Erfüllt das lokale Recht die genannten Garantien nicht, muss der Datenexporteur weitere technische, organisatorische und rechtliche Massahmen treffen. Kann durch solche Massnahmen der fehlende Schutz nicht ausgeglichen werden, folgt daraus, dass die Datenbekanntgabe ins Ausland ausgesetzt bzw. beendet wird.

Nach der Handlungsanleitung des EDÖB soll der Datenexporteur als gutgläubig gemäss Art. 3 Abs. 1 ZGB gelten, soweit er Daten in einen Staat übermittelt, der auf der Staatenliste als ein solcher mit angemessenem Datenschutzniveau aufgeführt wird. Hierbei soll es sich allerdings um eine widerlegbare Vermutung handeln. So soll der verantwortliche Datenexporteur bei der Erfassung und Analyse des Datentransfers alle nötigen Abklärungen vornehmen müssen, wie z.B. Einholen von unabhängigen Rechtsgutachten, u.a. zu folgenden Aspekten:

- Geltende Rechtsvorschriften im Zielland;
- Praxis der Verwaltungsbehörden und Gerichtsbehörden;
- Rechtsprechung.

Verbindlichkeit des Entscheids des Bundesrats zur Angemessenheit des Datenschutzes (Klarstellung in Art. 8 Abs. 1 Satz 2 E-VDSG)

Die durch den EDÖB vorgeschlagene Prüfung der obenstehenden Garantien durch den Datenexporteur muss sich aufgrund einer positiven Entscheidung des Bundesrats hinsichtlich der Angemessenheit des Datenschutzes in einem Drittstaat erübrigen. Dies folgt bereits daraus, dass ohne die Vorlage solcher Garantien nicht von einem angemessenen Datenschutz ausgegangen werden kann.

Eine zusätzliche Einzelfallprüfung und die damit einhergehende Beurteilung und Entscheidung zur jeweiligen (ausländischen) Rechtsordnung des Importstaates, hinsichtlich hinreichender Transparenz und Rechtsschutz für die betroffenen Personen durch den Datenexporteur, erscheint darüber hinaus aus Praktikabilitätsgründen weder als durchführbar noch als zielführend.

Denn einerseits sind die relevanten Rechtsgrundlagen, Rechtsprechung sowie insbesondere die Behördenpraxis für (geheime) Zugriffe nicht einheitlich kodifiziert und/oder öffentlich zugänglich. Der Bundesrat und speziell das EDA und das EJPD verfügen hier über die besten Quellen und Kenntnisse. Andererseits wäre eine solche Beurteilung als unverhältnismässig aufwändig zu werten, da diese eine Momentaufnahme widerspiegelt, die einem raschen Wandel unterliegen kann. Folglich könnte ein Verantwortlicher gar nicht innert vertretbarer Zeit adäquat auf Änderungen reagieren und sofortige neue Dispositionen treffen.

Darüber hinaus würde der Umstand, Unternehmen als Datenexporteure mit der Aufgabe zu betrauen, die Angemessenheit der Rechtsordnungen des Importstaates zu untersuchen und zu beurteilen, Art. 16 revDSG i.V.m. Art. 8 E-VDSG widersprechen. Diese Normen legen fest, dass die Angemessenheitsprüfung und die damit einhergehende Entscheidung vom Bundesrat und nicht von den datenexportierenden Stellen vorgenommen werden muss. Sollte nicht einheitlich der Bundesrat, sondern die datenexportierenden Verantwortlichen solche Beurteilungen vornehmen, sind unterschiedliche Ergebnisse hinsichtlich bestimmter Länder und Datenverarbeitungen vorprogrammiert. Dies würde im Ergebnis trotz viel Aufwand keine Rechtssicherheit schaffen. Die Liste des Bundesrats verlöre dadurch jeden Sinn.

Um eine faktische Aushöhlung der Feststellungskompetenz des Bundesrates sowie unterschiedliche Ergebnisse der Bewertung und eine damit einhergehende Rechtsunsicherheit zu vermeiden, muss deshalb auf Stufe E-VDSG ausdrücklich geklärt werden, dass sich die Verantwortlichen als Datenexporteure auf den Entscheid des Bundesrates zur Angemessenheit verlassen dürfen und keine zusätzlichen Abklärungen treffen müssen.

Daher soll zur Klarstellung **ein neuer Satz 2 in Art. 8 Abs. 1** E-VDSG eingefügt werden.

Formulierungsvorschlag
1 Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~ muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen~~t werden~~:
(a-~~e~~) …
Die Verantwortlichen dürfen sich auf den Entscheid des Bundesrates zur Angemessenheit des Datenschutzes nach Satz 1 verlassen und müssen keine zusätzlichen Abklärungen treffen.

Staaten oder internationale Organe ohne angemessenen Datenschutz (Klarstellung in Art. 8 Abs. 7 E-VDSG)

Alle nicht auf der Liste des Bundesrates aufgeführten Länder gelten per se als Länder mit nicht angemessenem Datenschutz. Wollen Verantwortliche in solche Länder Personendaten versenden bzw. dort bearbeiten (lassen), müssen sie selbst abklären, ob ein angemessener Datenschutz gegeben ist oder andernfalls ergänzend geeignete und angemessene Zusatzmassnahmen treffen. Das Urteil Schrems II des EuGHs generiert entgegen den Leitlinien des EDÖB vom 18. Juni 2021 in diesem Zusammenhang keine zusätzliche Liste von Ländern mit besonderem Risiko. Dies schon deshalb, weil sachlogisch bei jedem Land mit nicht angemessenem Datenschutz damit zu rechnen ist, dass spezifische Behörden und Stellen wie z.B. Geheimdienste ungefragt Einsicht in die betreffenden Daten nehmen und deshalb auch vom Urteil Schrems II erfasst sind. Eine solche Liste von Ländern mit hochgradig nicht angemessenem Datenschutz dürfte auch aus politischen Gründen nicht opportun sein, da sie wichtige internationale Beziehungen der Schweiz nachhaltig gefährden dürfte. Dies ist in Art. 8 E-VDSG im Sinne einer notwendigen Präzisierung klarzustellen, um obgenannte Leitlinien des EDÖB zu entkräften, sachlogisch in einem neuen Abs. 7.

Sollte an der durch den EDÖB vorgeschlagenen zusätzlichen Prüfung der obenstehenden Garantien, welche aus einer entsprechenden Auslegung der Schrems-II-Rechtsprechung des EuGHs resultiert, festgehalten werden, müsste die Prüfung dieser Garantien sachlogisch ebenfalls einheitlich durch den Bundesrat erfolgen. Dies auch deshalb, weil die Abgrenzung zwischen «nicht angemessen» und «hochgradig nicht angemessen» zwingend Wertungen beinhaltet, welche gesamthaft einheitlich von einer kompetenten Stelle anzuwenden sind. Nur dadurch wird ein in sich stimmiges Regelungssystem für die gesamte Thematik geschaffen, welches statt Verwirrung tatsächlich Rechtssicherheit schaffen würde. Andernfalls ergäben sich kontraproduktive Widersprüche zwischen der Liste des Bundesrates und den Zusatzlisten der Verantwortlichen. Als Folge davon würde die bereits vorstehend skizzierte Rechtsicherheit (oben Ziff. 2.2) trotz viel Aufwand sogar noch weiter erhöht.

Eine Einzelfallprüfung und eine damit einhergehende Beurteilung und Entscheidung zur jeweiligen (ausländischen) Rechtsordnung des Importstaates hinsichtlich hinreichender Transparenz und Rechtsschutz für die betroffenen Personen durch den Datenexporteur erscheint aus Praktikabilitätsgründen weder als durchführbar noch als zielführend.

Nach alledem ist zur Klarstellung ein **neuer Absatz 7 in Art. 8 E-VDSG** einzufügen.

Formulierungsvorschlag
[…]
7) Werden Personendaten ins Ausland in einen Staat oder ein Gebiet ohne angemessenen Datenschutz bekanntgegeben, können ergänzende Massnahmen zu den Garantien gemäss Art. 16 Absatz 2 Buchstabe b und c DSG erforderlich sein, um einen geeigneten Datenschutz zu gewährleisten. Der Bundesrat stellt fest, ob ergänzende Massnahmen erforderlich sind. Die betroffenen Staaten und Gebiete sind im Anhang 1a aufgeführt. Der Entscheid des Bundesrates bezüglich der Erforderlichkeit ergänzender Massnahmen ist verbindlich.

Artikel 9 (Datenschutzklauseln und spezifische Garantien)

Antrag:
Zumindest Abs. 1 lit. d, e, f, h und j sollen gestrichen werden. Lit. a soll um den Grundsatz der Transparenz ergänzt und in lit. g muss der «berechtigte Empfänger» durch den «Empfänger» ersetzt werden.

Begründung:

- Die von Art. 9 E-VDSG gestellten Anforderungen sind nicht erforderlich. Der EDÖB muss sie ohnehin prüfen. Zudem erreichen sie ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Zwar sind diese Anforderungen für das Ziel des Datenschutzes konsequent, sie verursachen aber hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden.
- In den Bearbeitungsgrundsätzen (lit. a) fehlt der Grundsatz der Transparenz.
- Das Erfordernis in lit. d und e, den Namen der Staaten oder der internationalen Organisationen zu nennen, denen Personendaten bekanntgegeben werden (soweit hiermit Weiterübermittlungen gemeint sind, was nicht klar ist), hat keine rechtliche Grundlage. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Auch die EU SCC beschränken sich darauf.
- Lit. f ist bereits mit dem Grundsatz der Verhältnismässigkeit in lit. a abgedeckt, und damit redundant und zu streichen.
- Lit. g geht zu weit, indem es die «berechtigten» Empfänger verlangt. Relevant sind die «Empfänger», also normalerweise die Parteien, welche den Vertrag abschliessen und damit bereits ersichtlich sind.
- Lit. h ist klarerweise unnötig und seine Anwendung wäre unverhältnismässig aufwendig. Andere bestehende Bestimmungen genügen, um die Garantien zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.
- In Abs. 2 sollte die Datenschutzklausel die Pflicht des Empfängers enthalten, die betroffenen Personen zu informieren. Es ist nicht Aufgabe des Auftragsverarbeiters, die betroffenen Personen zu informieren; dies ist Aufgabe des Verantwortlichen.

Aus diesen Ausführungen folgt überdies, dass der Anforderungskatalog in Art. 9 Abs. 1 E-VDSG entweder anzupassen ist, um unterschiedliche Konstellationen abzudecken (Verantwortlicher, Auftragsbearbeiter) und das Wort «mindestens» durch «je nach den Umständen» zu ersetzen ist.

Das DSG schreibt – wie die DSGVO – kein proaktives «Sicherstellen» der Einhaltung der Garantien durch den Verantwortlichen vor. Ein Eingreifen in Fällen, in welchen ein solches «Nicht-Einhalten» und damit eine Verletzung der Vertragspflichten eintritt, ist jedoch eine Reaktion durch den Verantwortlichen selbstverständlich, und kann entsprechend auch in Art. 9 Abs. 2 in die Verordnung aufgenommen werden.

Demnach ist Art. 9 E-VDSG wie folgt anzupassen:

Formulierungsvorschlag:
1) Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen je nach den Umständen ~~mindestens die~~ folgende~~n~~ Punkte regeln:
a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung, ~~und~~ der Richtigkeit und der Transparenz;
b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen;
c. die Art und den Zweck der Bekanntgabe von Personendaten
~~d. die Namen der Staaten, in die Personendaten bekanntgegeben werden;~~
~~e. die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden;~~
~~f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;~~
g. die Modalitäten der Weitergabe von ~~zur Bearbeitung der~~ Daten ~~berechtigten~~ an Empfängerinnen und Empfänger;
~~h. die Massnahmen zur Gewährleistung der Datensicherheit;~~
i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;
~~j. die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren;~~
k. […]
2) Der Verantwortliche muss angemessene Massnahmen treffen, ~~um sicherzustellen, dass~~ wenn die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien nicht einhält
3) […]

Artikel 10 (Standarddatenschutzklauseln)

Antrag:
Der Empfänger kann nicht verpflichtet werden, «die schweizerischen Datenschutzvorschriften» einzuhalten. Das ist im Erläuterungsbericht klarzustellen.
Und
Ersetzen des Begriffs «Sicherstellung» durch «darauf hinwirken».
Und
Präzisierung, dass sich die Angemessenheit der geforderten Massnahmen nach den Umständen im konkreten Einzelfall richte und die Anforderungen insb. dann höher seien, wenn es sich um besonders schützenswerte Personendaten handle.

Begründung:
Im Erläuterungsbericht (S. 28) ist festgehalten, dass der Empfänger verpflichtet werden müsse, «die schweizerischen Datenschutzvorschriften» einzuhalten. Das ist unzutreffend; er muss die Standardklauseln einhalten, nicht jedoch das Schweizer Datenschutzrecht. So verlangt auch Art. 6 Abs. 2, dass der Auftragsbearbeiter «gleichwertige» Bestimmungen einhalten muss.

Der Exporteur kann nicht «sicherstellen», dass der Empfänger die Standarddatenschutzklauseln beachtet; er kann nur, aber immerhin, darauf hinwirken.

Dies ist in den Erläuterungen (S. 28) unter Hinweis auf das BJ entsprechend festgehalten und sollte zur Klarstellung auch in die Verordnung einfliessen.

Der risikobasierte Ansatz bei der Beurteilung von Datentransfers in Länder ohne angemessenen Datenschutz auf Grundlage der SCC ist zu bejahen. Allerdings ist dieser Ansatz mit Blick auf die Praxishinweise der EU-Behörden keinesfalls selbstverständlich. Entsprechend bedarf es einer Klarstellung in der Verordnung zur Schaffung von Rechtssicherheit.

Formulierungsvorschlag:
1 Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Abs. 2 Buchstabe d DSG ins Ausland bekannt, so ~~trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.~~ trägt er in angemessener Weise Sorge für deren Einhaltung.

Und
Klarstellung im Erläuterungsbericht, dass der Empfänger nicht verpflichtet werden muss, «die schweizerischen Datenschutzvorschriften» einzuhalten.

2. Kapitel: Pflichten der Verantwortlichen ~~und des Auftragsbearbeiters~~

Da die Pflichten des Auftragsbearbeiters aus Sicht der Wirtschaft dringend gestrichen werden sollten, muss der Titel von Kapitel 2 angepasst werden.

Artikel 13 (Modalitäten der Informationspflicht)

Antrag:
1. Streichung des Auftragsverarbeiters.

Und
2. Ergänzung der Möglichkeit eine Information auch elektronisch zur Verfügung zu stellen.

Und
3. Streichung der unpräzisen Vorgaben für eine angemessene Information und Streichung der unklaren Anforderungen an Piktogramme.

Begründung:
1. Die Informationspflicht gegenüber den betroffenen Personen kann nur den Verantwortlichen treffen. Die vorgeschlagene Regelung steht im diametralen Widerspruch zum neuen DSG (Art. 19 revDSG) (!) und der DSGVO (Art. 13 und 14). In beiden Gesetzen trifft die Informationspflicht – selbstverständlich - nur den Verantwortlichen. Der Auftragsbearbeiter muss und kann nicht informieren, und er darf es auch gar nicht, ausser auf Weisung und in Vertretung des Verantwortlichen. Im Übrigen ist diese Pflicht strafbewehrt (Art. 60 revDSG), so dass auf diesem Weg auch die Strafbarkeit des Auftragsverarbeiters bzw. der für ihn handelnden Personen eingeführt würde. Dafür bräuchte es aus rechtstaatlichen Gründen zwingend ein Gesetz im formellen Sinn, was die VDSG nicht ist.
   Es ist zudem falsch, dass die Pflichtangaben «mitzuteilen» sind. Es geht bei der Datenschutzinformation nicht um eine Mitteilung wie bei bestimmten rechtgeschäftlichen Erklärungen, die dem Empfänger zugehen müssen (vgl. z.B. Art, 40e Abs. 4, Art. 176 Abs. 2 oder Art. 269d OR), sondern darum, eine bestimmte Situation – die Bearbeitung – nach aussen erkennbar zu machen. Vergleichbar ist dies mit der Deklaration von Konsumenteninformationen (vgl. Art. 1 lit. a KIG). Bei Art. 13 Abs. 1 E-VDSG ist deshalb von «zur Verfügung stellen» zu sprechen anstelle von «mitteilen».
2. Das revDSG sieht nicht vor, dass die Betroffenen die «wichtigsten Informationen» auf der «ersten Kommunikationsstufe» erhalten müssen (vgl. aber Erläuterungen, S. 30). Vielmehr hält revDSG Art. 19 Abs. 1 fest, die Information müsse «angemessen» erfolgen. Daraus folgt, dass die Mitteilung von den jeweiligen Umständen abhängig ist. Dabei sind auch Informationsinteresse und die Erwartungen des Betroffenen zu

berücksichtigen: Während er damit rechnen mag, dass sich in einem Vertrag ein Hinweis auf die Datenschutzerklärung findet, ist ein solcher auf Visitenkarten, E-Mails oder Briefpapier nicht üblich. Sollte sich eine Person ausnahmsweise dafür interessieren, kann ihr ohne weiteres zugemutet werden, z.B. die Webseite des betreffenden Unternehmens zu konsultieren. Darum darf es nicht erforderlich sein, in Alltagssituationen – wie bei einer Terminvereinbarung am Schalter – explizit auf die Datenschutzerklärung hinweisen zu müssen. Dabei ist der Standard «auf Papier oder elektronisch zur Verfügung stellen» zu wählen, welcher in neueren Gesetzen wie z.B. FIDLEG bereits genutzt wurde. Zudem wäre ohnehin unklar, welches die «wichtigsten Informationen» sind.

3. Weil Piktogramme ohnehin nur ergänzend verwendet werden dürfen, sind daran keine zusätzlichen Anforderungen zu stellen. Zumal aufgrund der Erläuterungen nicht klar ist, was mit «maschinenlesbar» gemeint ist.

Formulierungsvorschlag
1. Der Verantwortliche ~~und der Auftragsbearbeiter teilen~~ stellt die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form ~~mit~~ auf Papier oder elektronisch zur Verfügung.
2. ~~Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~

Artikel 15 (Information bei der Bekanntgabe von Personendaten)

Antrag:
Ersatzlos streichen.

Begründung:
Art. 15 E-VDSG statuiert völlig neue formale zusätzliche Modalitäten und Zusatzpflichten in Zusammenhang mit der Bekanntgabe von Daten an Dritte, welche strikt regelbasiert ohne Differenzierungsmöglichkeit in jedem Fall anwendbar sein sollen. Hierzu findet sich im revDSG keine gesetzliche Grundlage. Im Gegenteil hat das Parlament die Bekanntgabe von Personendaten an Dritte bereits auf Gesetzesstufe an verschiedenen Stellen ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt (vgl. namentlich Art. 16 ff. revDSG). Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen.

Die Regelung würde inhaltlich zu massiven Zusatzanforderungen bei jeder Art von Kommunikation in Zusammenhang mit Personendaten, z.B. bei jedem einzelnen E-Mail, führen. Damit würden an übliche und vernünftige Kommunikation, selbst solche ohne erkennbare datenschutzrechtliche Risiken, völlig überrissene Anforderungen gestellt. Im operativen Alltag würden damit etablierte, übliche und vernünftige Kommunikationsmittel wie z.B. E-Mail de facto gänzlich verhindert. Solche Anforderungen stehen in vollständigem Widerspruch zu den Anstrengungen des Bundesrats, Digitalisierung und Innovationskraft im Interesse des Wirtschaftsstandorts Schweiz zu fördern.

Dementsprechend finden sich auch im EU-Recht, auf welches sich der Erläuterungsbericht zu Unrecht beruft, keine solchen Pflichten für private Datenbearbeiter. Art. 15 E-VDSG ist mithin ein für das wesentliche Regulierungsziel EU-Äquivalenz kontraproduktiver Swiss Finish.

Somit ist die Regelung Art. 15 **am besten gänzlich zu streichen, zumindest** aber ausdrücklich **auf Bundesorgane einzugrenzen**.

Sofern die Regelung nicht gänzlich gestrichen wird, ist zudem auch hier der Auftragsbearbeiter jedenfalls nicht Adressat der Informationspflicht und ist deshalb zu streichen. Der Auftragsbearbeiter verfügt weder über die entsprechenden Angaben noch ist er zu einer solchen Mitteilung befugt, es sei denn auf Weisung und in Vertretung des Verantwortlichen.

Artikel 16 (Information über die Berichtigung, Löschung und Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten)

Antrag:
Ersatzlos streichen.

Begründung:
Die Pflicht wurde im Rahmen der Vernehmlassung zum revDSG gestrichen und darf nun nicht über die VDSG wieder eingeführt werden. Zudem besteht keine Notwendigkeit, da der Verantwortliche bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten hat, ebenso wie die Empfänger von Personendaten.

Darum ist Art. 16 E-VDSG **zu streichen**.

Artikel 17 (Überprüfung einer automatisierten Einzelentscheidung)

Antrag:
Ersatzlos streichen.

Begründung:
Dieser Artikel stellt unseres Erachtens einen Eingriff in die Privatrechtsautonomie dar und kann daher nicht auf Verordnungsstufe verankert werden.

Zudem geht die Regelung von falschen rechtlichen Voraussetzungen aus. Ein generelles Diskriminierungsverbot gibt es nicht. Soweit es direkt aus Grundrechten der Verfassung abgeleitet werden sollte, wäre dies unzulässig, da es keine direkte Drittwirkung verfassungsmässiger Rechte gibt. Eine Diskriminierung wird rechtlich erst dann kritisch, wenn sie rein subjektiv ohne sachlich überzeugende Abgrenzungskriterien erfolgt. All dies ist aber schon deshalb nicht auf Stufe E-VDSG zu regeln, weil das Thema allgemeiner Natur ist und in sämtlichen Rechtsmaterien gleichermassen eine Rolle spielt. Nur schon die etablierte bundesgerichtliche Praxis zum Thema gibt ausreichende Rechtssicherheit.

Eine weitere Präzisierung von Art. 21 revDSG auf Stufe E-VDSG ist weder sinnvoll noch nötig und mangels gesetzlicher Grundlage auch nicht zulässig. Das Parlament hat die Anforderungen an die Informationspflichten bei automatisierten Einzelentscheiden in Art. 21 revDSG bereits ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt. Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen.

Nach alledem gleichwohl eine solche Regel in die E-VDSG einzuführen würde unnötigerweise erhebliches Potential für missbräuchliche Klagen gegen Verantwortliche produzieren, welche sich effektiv absolut korrekt und gesetzeskonform verhalten.

Art. 17 E-VDSG sollte demnach **ersatzlos gestrichen werden**.

Artikel 18 (Form und Aufbewahrung der Datenschutz – Folgeabschätzung)

Antrag:
Die Aufbewahrungsfrist ist zu streichen und «schriftlich» zu präzisieren.

Begründung:
Wie in anderen modernen Gesetzen auch sollte der Begriff der Schriftlichkeit dahingehend präzisiert werden, dass auch andere Formen erfasst werden, die den Nachweis durch Text ermöglichen.

Die Aufbewahrungspflicht sollte im zweiten Satz von Art. 18 E-VDSG mangels gesetzlicher Grundlage im revDSG gestrichen werden. Ausserdem besteht unseres Erachtens aufgrund des Grundsatzes der Verhältnismässigkeit der Datenbearbeitung sowie der Datenminimierung kein Grund, eine Datenschutz-Folgenabschätzung während zwei Jahren nach Beendigung der Datenbearbeitung aufzubewahren. Schliesslich widersprechen die Ausführungen im Erläuterungsbericht dem nemo-tenetur-Grundsatz, sollten die Datenschutz-Folgenabschätzung zu Beweiszwecken gegen den Verantwortlichen aufbewahrt werden.

Sollte an den zwei Jahren festgehalten werden, müsste mindestens die Ergänzung «während mindestens zwei Jahren» oder «für einen angemessenen Zeitraum» eingesetzt werden, sodass eine allfällige längere Aufbewahrung der Daten nicht als datenschutzwidrig gilt.

Formulierungsvorschlag:
1 Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in anderer durch Text nachweisbarer Form festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~

Artikel 19 (Meldung von Verletzungen der Datensicherheit)

Antrag:

1. Lit. e und lit. f sind zu präzisieren.
2. Streichung der über das Gesetz hinausgehenden generellen Pflicht, die betroffene Person zu informieren.
3. Streichung der gesetzlich nicht vorgesehenen Dokumentationspflicht nach VDSG Art. 19 Abs. 5.
4. Anpassung Erläuterungsbericht: Die Auslegung des Begriffs «voraussichtlich» ist falsch und zu korrigieren.

Begründung:

1. Lit. e ist falsch formuliert. Die «allfälligen Risiken» beinhalten bereits die Folgen für die betroffenen Personen. Richtig müsste es heissen: «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht». Auch in lit. f muss nicht von den «Folgen», sondern vom «Risiko» die Rede sein. Gemildert werden kann entweder das Schadensausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem «Risiko» entspricht). Bei Bst. f ist zudem zu präzisieren, dass es nur um Massnahmen gehen kann, welche der Verantwortliche tatsächlich ergriff («gegebenenfalls»).
2. Art. 19 Abs. 2 E-VDSG geht über Art. 20 Abs. 4 revDSG hinaus. Während das Gesetz eine Information der betroffenen Person nur vorschreibt, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt, sieht die Verordnung vor, dass der Verantwortliche den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mitteilt. Zusätzlich besteht keine gesetzliche Grundlage (Mindestangaben, Dokumentationspflicht) und es entsteht ein Swiss Finish (Angabe von Zeitpunkt und Dauer der Verletzung)

3. Die Dokumentationspflicht gemäss Art. 19 Abs. 5 E-VDSG entbehrt einer gesetzlichen Grundlage und sollte folglich ersatzlos gestrichen werden. Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen Swiss Finish darstellt. Falls an der Dokumentationspflicht festgehalten werden sollte, ist zu präzisieren, dass nur meldepflichtige Verletzungen aufzubewahren sind.
4. «Voraussichtlich» heisst nicht, dass «in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, eine Meldung erfolgen muss» (so die Erläuterungen, S. 32). Der Begriff «voraussichtlich» setzt vielmehr voraus, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko führt. Der Erläuterungsbericht sollte so berichtigt werden, dass in Fällen, wo das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, nicht gemeldet werden muss, sondern nur dann, wenn die Verletzung der Datensicherheit höchstwahrscheinlich zu einem hohen Risiko führt.

Formulierungsvorschlag:
1 Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit:
a. die Art der Verletzung;
b. soweit möglich den Zeitpunkt und die Dauer;
c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;
d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;
e. die Folgen~~, einschliesslich der allfälligen Risiken,~~ für die betroffenen Personen, von welchen ein hohes Risiko ausgeht;
f. gegebenenfalls welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder ~~die Folgen~~ das Risiko zu mildern;
g. den Namen und die Kontaktdaten einer Ansprechperson.
2 Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.
3 ~~Der~~ Falls der Verantwortliche verpflichtet ist, die ~~teilt den~~ betroffenen Personen zu informieren, so teilt er ihnen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit.
4 […]
~~5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.~~

3. Kapitel: Rechte der betroffenen Person

Artikel 20 (Modalitäten)

Antrag:

1. Die Auskunftserteilung sollte nicht nur schriftlich, sondern auch in einer anderen durch Text nachweisbaren Form möglich sein.
2. Aufnahme der Präzisierung, dass der Begriff «Daten als solche» insbesondere auch eine Auskunft in aggregierter Form zulässt.
3. Ergänzung bzw. Umformulierung von Abs. 3
4. Dokumentationspflicht nach Art. 20 Abs. 5 ist zu streichen.

Begründung:

1. In den Erläuterungen (S. 34) wird festgehalten: «Es kann hier ferner präzisiert werden, dass zur schriftlichen Form auch die elektronische Form gehört.» Diese Präzisierung ist in die Verordnung aufzunehmen.

2. In den Erläuterungen (S. 35) wird ausgeführt: «Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Die mündliche Mitteilung von Informationen, zum Beispiel am Telefon, ist ebenfalls möglich, sofern die betroffene Person eingewilligt hat.» Es besteht im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten bzw. Unterlagen. Vielmehr ist die Mitteilung nach entsprechender Debatte vom Gesetzgeber bewusst beschränkt worden auf die «bearbeiteten Personendaten als solche» (Art. 25 Abs. 2 lit. b revDSG). Damit soll namentlich auch die Auskunft in aggregierter Form ermöglicht werden. Dies sollte zwecks Präzisierung in der Verordnung verankert werden.
3. Betreffend Art. 20 Abs. 3 E-VDSG haben die Mitglieder von economiesuisse zwei verschiedene Vorgehensweisen, um eine Anpassung im Sinne der Wirtschaft vorzunehmen. Einige Mitglieder sprechen sich für eine Streichung des Absatzes aus, während Andere eine Streichung unterstützen würden, aber alternativ für eine Umformulierung plädieren.

   Option 1: Streichung

   Für eine komplette Streichung spricht, dass das Gesetz bereits eine Auskunft an die betroffene Person vorschreibt und auch den Umfang und die Art dieser Auskunft bereits klar und deutlich definiert. Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Eine weitere Pflicht des Verantwortlichen, einer betroffenen Person diese Auskunft auch noch «verständlich» zu machen, entbehrt einer gesetzlichen Grundlage. Nachdem das Gesetz den Mindestumfang der Auskunft im Detail beschreibt, ist diese zusätzliche Anforderung in der Verordnung auch gar nicht notwendig, dürfte eine Auskunft, welche den gesetzlichen Vorgaben entspricht, regelmässig für jeden Durchschnittsadressaten verständlich sein. Diese Verordnungsbestimmung schiesst zudem über das Ziel hinaus, vgl. Begründung in der Wegleitung: «Werden Personendaten in einer technischen Form geliefert, die für die betroffene Person nicht lesbar und/oder nicht verständlich ist, muss der Verantwortliche imstande sein, ihr ergänzende Erläuterungen zu geben, beispielsweise mündlich.»

   Option 2: Umformulierung

   Art. 20 Abs. 3 E-VDSG verlangt, dass die Auskunft verständlich sein muss. Dies bedeutet nicht, dass der Verantwortliche der um Auskunft ersuchenden Person die Datensätze oder darüber hinaus sogar die damit einhergehenden Abläufe und Geschäftsmodelle erklären muss. Dies könnte im Einzelfall je nach Person mit enormem und unverhältnismässigem Aufwand verbunden sein und wäre je nach Person u.U. gleichwohl untauglich. Zudem könnte eine solche Regelung auch dazu missbraucht werden, das Verfahren und damit den Aufwand für den Verantwortlichen ohne sachlichen Grund «künstlich» zu verlängern.

   Vielmehr muss ausreichend sein, die herauszugebenden Daten so aufzubereiten und darzustellen, dass sie geordnet sind und dadurch unter Anwendung eines objektivierten Masstabes nach Treu und Glauben verständlich sind oder sein müssen. Ob die betroffene Person diese Darstellung im konkreten Fall tatsächlich versteht, kann nicht relevant sein, geht es doch beim datenschutzrechtlichen Auskunftsbegehren nur darum, die bearbeiteten Daten mitzuteilen. Dies entspricht dem Kern des Auskunftsanspruchs, welcher die effektive Herausgabe der relevanten Daten sicherstellt. Darüber hinaus besteht keine Pflicht des Verantwortlichen, die Daten, deren Zweck oder – damit zusammenhängend – die Art der Datenhaltung oder sogar die Geschäftsabläufe zu erläutern. Solches ist schon deshalb abzulehnen, weil dadurch der Aufwand unermesslich und im Einzelfall sogar «never ending» werden könnte. Beispielsweise können die im Rahmen einer klinischen Studie bearbeiteten Daten oder technische Logdaten für die betroffene Person unverständlich sein. Müssen diese zuerst so dargestellt werden, dass sie für die betroffene Person verständlich sind, kann dies oft nicht innerhalb von 30 Tagen erfolgen. Damit würde der Grundsatz der Auskunftserteilung innert 30 Tagen entgegen der gesetzlichen Absicht regelmässig zur Ausnahme.

   Will die auskunftsberechtigte Person mehr über solche über den eigentlichen Herausgabeanspruch hinaus gehende Verhältnisse erfahren, muss sie sich an einen Rechtsanwalt oder Wirtschaftsfachmann halten, nicht an den Verantwortlichen. Demzufolge ist Abs. 3 zusätzlich dahingehend zu klären, dass über die eigentliche «geordnete» Datenherausgabe «keine zusätzlichen Erläuterungen erforderlich» sind.

   Da die Aktivität und die damit einhergehende Verständlichkeit der Auskunft vom Verantwortlichen ausgeht

und von diesem gesteuert werden kann und muss, macht es Sinn, den Verantwortlichen hier bei Abs. 3 mit Bezug auf die Formulierung in den Aktiv-Modus zu setzen.

4. Die Dokumentationspflicht nach Art. 20 Abs. 5 entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen Swiss Finish darstellt. Die Regelung ist ferner unnötig, da aufgrund der Beweislast ohnehin im Interesse des Verantwortlichen, mit Dokumentation den Nachweis erbringen zu können.

Formulierungsvorschlag
1-2 […]
3 ~~Die Auskunft muss für die betroffene Person verständlich sein.~~ Der Verantwortliche muss die Auskunft geordnet vornehmen. Zusätzliche Erläuterungen sind nicht erforderlich.
Oder
~~3 Die Auskunft muss für die betroffene Person verständlich sein.~~
4 Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.
~~5 Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.~~

Artikel 21 (Zuständigkeit)

Antrag:

1. Streichung Abs. 1 Satz 2
2. Konkretisierung Abs. 2

Begründung:

1. Der erste Satz von Art. 21 Abs. 1 E-VDSG ist nicht zu beanstanden. Der zweite Satz stellt demgegenüber eine Forderung auf, welche im operativen Alltag regelmässig gar nicht erfüllt werden kann. In manchen Konstellationen ist für einen Verantwortlichen weder klar noch eindeutig ersichtlich, inwieweit für einen bestimmten Sachverhalt ein anderer Verantwortlicher zuständig sein soll und wer dies gegebenenfalls ist. In vielen Fällen kann ein Verantwortlicher deshalb der Pflicht, das Begehren an den zuständigen Verantwortlichen weiterzuleiten, naturgemäss gar nicht nachkommen. In unklaren Fällen ein Auskunftsbegehren an andere, vermeintlich zuständige Verantwortliche, weiterzuleiten, würde dem Datenschutz geradezu entgegenlaufen, erhielten doch auf diese Weise womöglich Personen Kenntnis vom Fall, welche gar nicht als Verantwortliche qualifiziert wurden. Einer fälschlicherweise um Auskunft ersuchten Person ist es auch nicht zuzumuten, abzuklären, wer an seiner Stelle Verantwortlicher sein könnte. Auch solche Abklärungen würden dem berechtigten Bedürfnis der um Auskunft ersuchenden Person nach Einhaltung des Datenschutzes gerade zuwiderlaufen.
2. Auftragsbearbeiter sind nicht darauf eingerichtet, Auskunft zu erteilen, weil sie keine entsprechende gesetzliche oder vertragliche Pflicht haben. Der Verweis auf eine Auskunftserteilung durch den Auftragsbearbeiter ist deshalb falsch und kann in der Praxis Probleme schaffen. Gemeint ist hier wohl vielmehr, dass Auftragsbearbeiter den Verantwortlichen bei der Auskunftserteilung unterstützen sollen, was in der Praxis ohnehin jeweils so vereinbart wird.
   Des Weiteren ist Art. 21 Abs. 2 E-VDSG verwirrlich, da er impliziert, dass der Auftragsbearbeiter selbst eine Auskunftspflicht hat, wenn er faktisch in der Lage sein sollte, eine Auskunft zu erteilen bzw. er das Auskunftsgesuch in einem solchen Fall nicht weiterleiten muss, auch wenn er es nicht beantwortet. Das kann

nicht sein. Im Gegenteil ist es dem Auftragsbearbeiter i.d.R. vertraglich untersagt, selbst Auskunft zu erteilen, wenn ein Auskunftsbegehren direkt bei ihnen eingehen sollte. Der letzte Halbsatz von Abs. « («sofern er nicht in der Lage ist, selbst Auskunft zu geben») ist zu streichen und durch die Formulierung "sofern er das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet» zu ersetzen.

Formulierungsvorschlag:
1. Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. ~~Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.~~
2. Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so ~~leitet der Verantwortliche das Begehren zur Erledigung an den Auftragsbearbeiter weiter,~~ unterstützt der Auftragsbearbeiter den Verantwortlichen bei der Erteilung der Auskunft, sofern er ~~nicht in der Lage ist, selbst Auskunft zu erteilen~~ das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet.

Artikel 22 (Frist)

Antrag:
Der Fristbeginn ist zu präzisieren.

Begründung:
Wenn aus dem Auskunftsbegehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, soll die Frist erst mit dieser Klarstellung zu laufen beginnen. Zudem ist klarzustellen, dass erst der Eingang des Begehrens beim Verantwortlichen fristauslösend ist und nicht etwa beim Auftragsbearbeiter, falls ein Betroffener das Begehren dem Auftragsbearbeiter zugestellt und dieser das Begehren dem Verantwortlichen weiterleitet.

Formulierungsvorschlag:
1 Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens beim Verantwortlichen erteilt. Erfordert das Begehren einer Präzisierung, welche Daten die betroffene Person wünscht, beginnt die Frist mit Zugang der Präzisierung beim Verantwortlichen zu laufen. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen.

Artikel 23 (Ausnahme von der Kostenlosigkeit)

Antrag:

1. Der Maximalbetrag von CHF 300.- ist zu streichen.
2. Der Fristbeginn sollte ergänzt werden, um die 30 Tage sicherzustellen.

Begründung:

1. Der Maximalbetrag von CHF 300.-- wird den tatsächlichen Verhältnissen und dem damit verbundenen Aufwand nicht ansatzweise gerecht. Sind z.B. zur Sicherstellung des Datenschutzes von Dritten umfangreiche Schwärzungen notwendig, kann dies im Einzelfall durchaus höhere Aufwendungen mit sich bringen. Art. 23 Abs. 2 E-VDSG sollte deshalb gestrichen werden, da die die angemessene Kostenbeteiligung bereits in Abs. 1 enthalten ist und keine weiteren Einschränkungen nötig sind.
2. Abs. 3 muss dahingehend angepasst werden, dass die in Abs. 1 geregelte Frist von 30 Tagen zur Auskunftserteilung nicht faktisch auf 20 Tage abgekürzt werden kann. Dies kann durch eine Ergänzung des Fristbeginns in Abs. 3 sichergestellt werden.

Formulierungsvorschlag:
1 Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden~~,~~ oder querulatorisch ist.
~~2 Die Beteiligung beträgt maximal 300Franken.~~
3 Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen. Die Frist zur Auskunftserteilung beginnt mit Ablauf der Rückzugsfrist.

4. Kapitel: Rechte der betroffenen Person

Artikel 25 (Datenschutzberaterin und Datenschutzberater)

Antrag:

1. Art. 25 Abs. 1 lit. b E-VDSG ist ersatzlos zu streichen. Dementsprechend kann Art. 25 Abs. 1 lit. a E-VDSG direkt in Abs. 1 integriert werden.
2. Das Interventionsrecht gemäss lit. b ist zur Vervollständigung einer konzeptionell in sich stimmigen «Good Governance» mit dem Eskalationsrecht in einer neuen lit. c zu ergänzen.

Begründung:

1. Die gesetzliche Regelung zur Funktion der Datenschutzberatung wird auf Verordnungsstufe eingeengt.
   Die Datenschutzberaterin oder der Datenschutzberater muss lediglich beratend Einfluss nehmen, damit der Verantwortliche die Datenschutzpflichten richtig anwendet (vgl. Art. 10 revDSG, insb. Abs. 2 lit. b). Bei der Formulierung von Art. 25 Abs. 1 lit. a E-VDSG bleibt mit der Formulierung «prüft» der Umfang der Prüfpflicht unklar. Die Funktion Datenschutzberatung kann jedenfalls nicht jede beim Verantwortlichen anfallende Datenbearbeitung prüfen. Der Verantwortliche kann aber in Absprache mit der Funktion Datenschutzberatung eine interne Governance schaffen, welche in geeigneter Form die internen Regeln zu diesem Thema festlegt. So sollte die Funktion Datenschutzberatung nur solche Datenbearbeitungen prüfen, welche ihr effektiv vorgelegt werden. Dies auch zum eigenen Schutz. Ausserhalb der Konsultationspflicht muss die Funktion Datenschutzberatung entsprechend ihrer Hauptfunktion nur allgemein beratend tätig sein. Zur Klarstellung dieser Verhältnisse ist – auch zum Schutz von Datenschutzberatenden, für welche keine spezifische interne Governance besteht – die in Art. 25 Abs. 1 Bst a genannte Prüfpflicht auf «ihm vorgelegte» Datenbearbeitungen einzugrenzen.
   Die Regelung von Art. 25 Abs. 1 Bst b E-VDSG widerspricht der Funktion Datenschutzberatung und überdies der Organisationsfreiheit des Verantwortlichen, wie genau die Pflichten gemäss revDSG unter Würdigung der konkreten Verhältnisse im Unternehmen personell, technisch und organisatorisch am besten erfüllt werden sollen. Insofern liegt ein nicht stufengerechter Eingriff in die Privatautonomie des Unternehmens vor.
   Ferner verletzt die Bestimmung das weltweit als Standard etablierte drei Linien Verteidigungsmodell, in dem es die Erkennung, Einhaltung und Korrektur von datenschutzrechtlichen Vorgaben einer einzelnen Funktion, namentlich der Datenschutzberaterin oder dem Datenschutzberater, auferlegt.
   Schliesslich macht die vorgeschlagene Regelung von Art. 25 Abs. 1 lit. b E-VDSG die übergeordnete Ausnahmeregelung von Art. 23 Abs. 4 revDSG obsolet oder anders gesagt: Art. 25 Abs. 1 lit. b E-VDSG ist gar nicht nötig, weil mit Art. 23 Abs. 4 revDSG bereits eine ausreichende, übergeordnete Regelung besteht.

   Nach alledem ist Art. 25 Abs. 1 lit. b E-VDSG ersatzlos zu streichen. Dementsprechend kann Art. 25 Abs. 1 lit. a E-VDSG direkt in Abs. 1 integriert werden, was die Regelung etwas kürzer macht (siehe folgender Formulierungsvorschlag).

2. Art. 25 Abs. 2 lit. b E-VDSG regelt zu Recht ein Interventionsrecht. Dies ist nötig, damit die oder der Datenschutzberater/in bei unternehmensinternen Prüfungen der Einhaltung datenschutzrechtlicher Regeln nicht nur den Worten bzw. den ihm zur Verfügung gestellten Dokumenten vertrauen muss, sondern – soweit sinnvoll und nötig – die Beschaffung zusätzlicher Informationen und Dokumente durchsetzen kann. Mit dieser Regelung bleibt Art. 25 Abs. 2 lit. b E-VDSG aber «auf halbem Weg» stehen. Stösst die Datenschutzberaterin oder der Datenschutzberater nämlich bei der Ausübung des Interventionsrechts auf Unstimmigkeiten und sind die Linienverantwortlichen nicht gewillt, entsprechend dem Ratschlag der Datenschutzberaterin oder des Datenschutzberaters Abhilfe zu schaffen, muss Letzterer oder Letzterem spiegelbildlich zum Interventionsrecht bzw. zur Vervollständigung des Gesamtprozesses überdies ein Eskalationsrecht zustehen. Ein solches Recht ist sachlogisch keine Pflicht. Die Datenschutzberaterin oder der Datenschutzberater erhält damit aber das notwendige Instrumentarium, zumindest im Fall komplexer Verhältnisse und besonders schwerwiegende Verstösse gegen Datenschutzpflichten notfalls, mithin als Ausnahme von der Regel, die Thematik im Rahmen und allenfalls in Absprache mit der Compliance-Organisation, soweit eine solche besteht, auf dem Linienweg nach oben zu eskalieren und auf diese Weise auf höherer Stufe zum Entscheid zu bringen bzw. bringen zu lassen, nötigenfalls bis zum höchsten Organ des Unternehmens, und damit klare Verhältnisse zu schaffen. Bei einfacheren Strukturen genügt es aber auch, wenn die Funktion Datenschutzberatung in wichtigen Fällen die höchsten Organe lediglich informiert. Andernfalls setzt sich die Datenschutzberaterin oder der Datenschutzberater gerade bei schwerwiegenden Verstössen gegen Datenschutzpflichten dem Risiko aus, mangels Eskalationsmöglichkeit im Schadensfall selbst haftbar zu werden, weil ihr oder ihm vorgeworfen wird, sich nicht hartnäckig genug eingesetzt zu haben. Art. 25 Abs. 2 ist somit mit einer lit. c zu ergänzen, welche ergänzend zum Interventionsrecht nach lit. b das Eskalationsrecht regelt.

Formulierungsvorschlag:
1 Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen ~~muss folgende Aufgaben wahrnehmen: a. Sie oder er~~ prüft die ihr oder ihm vorgelegten Bearbeitungen von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass rechtliche Datenschutzvorschriften verletzt wurden.
~~b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.~~
2 Der private Verantwortliche muss der Datenschutzberaterin oder dem Datenschutzberater:
a. die notwendigen Ressourcen zur Verfügung stellen;
b. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.
c. das Recht einräumen, in wichtigen Fällen die höchsten Organe zu informieren.

Artikel 26 (Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten)

Antrag:
Es ist zu präzisieren, dass sich die allfällige Pflicht eines KMU zur Führung eines Verzeichnisses nicht auf sämtliche Bearbeitungen erstreckt, sondern auf diejenigen Bearbeitungen beschränkt ist, welche die Voraussetzung(en) triggern.

Begründung:
Der Bundesrat hat gemäss Art. 12 Abs. 5 revDSG Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses vorzusehen für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und deren Datenbearbeitung ein «geringes Risiko» mit sich bringt. Gemäss E-VDSG 26 bedeutet ein geringes Risiko, dass weder «umfangreich besonders schützenswerte Personendaten bearbeite» werden, noch «ein Profiling mit hohem Risiko durchgeführt» wird. Alle anderen Bearbeitungen bringen im Umkehrschluss ein geringes Risiko mit sich.

Durch Präzisierung, dass sich die Pflicht zur Führung eines Verzeichnisses ausschliesslich auf diejenigen Bearbeitungen erstreckt, welche die Voraussetzung triggern, kann sowohl dem Schutz der betroffenen Personen als auch den Bedürfnissen der KMU angemessen Rechnung getragen werden (vgl. auch das Positionspapier des EDSA zu Art. 30 Abs. 5 DSGVO).

Es ist ferner zu präzisieren, dass das Verzeichnis nicht schriftlich, sondern auch in anderer Form, die den Nachweis durch Text ermöglicht, z.B. elektronisch, geführt werden kann. Damit ist klargestellt, dass das Verzeichnis auch elektronisch geführt werden kann.

Formulierungsvorschlag:
1 Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:
a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet.
b. Es wird ein Profiling mit hohem Risiko durchgeführt.
2 Ist eine Voraussetzung nach Abs. 1 lit. a und/oder b erfüllt, so ist die Verzeichnispflicht auf diejenige Bearbeitung bzw. diejenigen Bearbeitungen beschränkt, welche dieser Voraussetzung bzw. diesen Voraussetzungen zugrunde liegen.
3 Das Bearbeitungsverzeichnis ist schriftlich, oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu führen.

7. Kapitel: Schlussbestimmungen

Antrag:
Das lückenhafte Übergangsregime auf Stufe des revDSG ist auf Verordnungsstufe mit zusätzlichen Übergangsbestimmungen zu ergänzen.

Begründung:
Für sämtliche neuen Pflichten, welche erheblichen Aufwand generieren, müssen angemessene Übergangfristen bestehen, zumal IT-gestützte Lösungen nötig sind.

Dabei ist zu berücksichtigen, dass die verschiedenen Regeln und Pflichten des gesamten Regelwerks (Gesetz samt Verordnung) gegenseitige Wechselwirkungen generieren. Die neuen Regeln bzw. Pflichten sind deshalb zusammen mit den unverändert weiter geltenden Regeln bzw. Pflichten zu einem in sich stimmigen Gesamtkonzept zu verschmelzen. Ein solches Gesamtkonzept kann sachlogisch erst nach Vorliegen der finalen Texte auf Gesetzes- und Verordnungsstufe erarbeitet, final festgelegt und umfassend in die IT-Sprache «übersetzt» werden. Erst danach kann mit dem Aufbau der IT-gestützten Lösung begonnen werden. Vor der «Go live»-Schaltung sind sodann die nach bewährten Standards vorgesehenen Tests durchzuführen. Parallel dazu sind auch die Mitarbeitenden entsprechend ihrer jeweiligen Funktion auszubilden und überdies die Verträge mit Lieferanten und Geschäftspartnern anzupassen.

Für alle diese notwendigen Aktivitäten ist gemäss etablierten Erfahrungswerten ein Zeitraum von rund 2 Jahren ab Vorliegen der finalen Gesetzes- und Verordnungstexte notwendig. Im Gegenzug stellt eine solche IT-gestützte Lösung die gleichförmige Anwendung sämtlicher Regeln innerhalb des gesamten Unternehmens sicher.

Aus den genannten Gründen hat die EU seinerzeit entschieden, für die Umsetzung der EU-DSGVO nicht Übergangsfristen für einzelne Regeln bzw. Pflichten, sondern pauschal 2 Jahre für das gesamte Regelwerk zuzugestehen.

In der Schweiz hat das Parlament für das revDSG eine andere Grundentscheidung getroffen (vgl. Art. 68-74 revDSG). Im Rahmen des parlamentarischen Prozesses liegt der Fokus naturgemäss auf den materiellen Regeln bzw. Pflichten. Das kam beim revDSG besonders deutlich zum Ausdruck, wurde doch über den konkreten Wortlaut einiger zentraler Bestimmungen wie z.B. zum Profiling (Art. 5 lit. f und g revDSG) buchstäblich bis zum Schluss heftig debattiert. Die Übergangsbestimmungen kommen deshalb im parlamentarischen Prozess regelmässig zu kurz, was beim revDSG in erhöhtem Mass der Fall war. Übergangsbestimmungen sollen zudem strikt nach sachlichen Kriterien festgelegt werden und nicht «Spielball» politischer Kompromisse sein. Deshalb hat es sich im schweizerischen Gesetzgebungsprozess inzwischen eingebürgert, falls notwendig ergänzende Übergansbestimmungen auf Verordnungsstufe festzulegen.

Im Zuge der DSG-Revision ist zumindest für folgende entweder neu eingeführten oder zumindest mit neuen Anforderungen konfrontierten Regeln bzw. Pflichten mit offensichtlich erheblichem Umsetzungsbedarf auf Gesetzesstufe keine Übergangsbestimmung festgelegt worden:

- Pflicht, eine angemessene Datensicherheit zu gewährleisten (Art. 8 revDSG i.V.m. Art. 1ff. E-VDSG);
- Pflicht zur Erstellung des Verzeichnisses der Datenbearbeitungstätigkeiten (Art. 12 revDSG);
- Pflicht, so rasch als möglich Meldung von Verletzungen der Datensicherheit zu erstatten (Art. 24 revDSG i.V.m. Art. 19 E-VDSG).

Gerade diese drei zentralen Pflichten können naturgemäss erst gestützt auf das Vorliegen eines umfassenden, in sich stimmigen Gesamtkonzepts sämtlicher Regeln bzw. Pflichten zielführend und final festgelegt werden.

Der finale Wortlaut der E-VDSG wird wohl erst gegen Ende des Jahres 2021 vorliegen. Unter Mitberücksichtigung des Umstandes, dass gestützt auf den Wortlaut des revDSG mit den Umsetzungsarbeiten zumindest schon begonnen werden konnte, ist nach dem Gesagten für die beiden vorgenannten Pflichten eine Übergangsfrist bis allermindestens 1. Juli 2023 notwendig, wobei die Aufrechterhaltung der Äquivalenz sichergestellt werden muss.

Formulierungsvorschlag:
Art. 48 ~~Inkrafttreten~~ Übergangsbestimmung betreffend das Verzeichnis der Bearbeitungstätigkeiten und der Meldung von Verletzungen der Datensicherheit
~~Diese Verordnung tritt am ... in Kraft~~. Art. 12 und 24 des Gesetzes sind erst ab 1. Januar 2023 zu erfüllen.

In der Folge würde Art. 48 E-VDSG (Inkrafttreten) neu zu Art. 49 E-VDSG.

Art. 48~~49~~ Inkrafttreten
Diese Verordnung tritt am ... in Kraft.

Eventualiter:
Alternativ zum neuen Art. 48 E-VDSG kann stattdessen das Inkrafttreten des ganzen Gesetzgebungspakets (revDSG und E-VDSG) nach hinten auf den 1. Juli 2023 geschoben werden (dynamisches Verhältnis zwischen Inkrafttreten und Übergangsfristen).

Da zwischen dem Abschluss des revDSG und der Vernehmlassung zur VDSG fast ein Jahr verstrichen ist, sollte die Dringlichkeit nicht mehr als Hauptargument einer raschen Inkraftsetzung genannt werden. Zudem brauchen die Unternehmen für die Umsetzung der Verordnung auch ausreichend Zeit. Dies vor allem auf Grund der zusätzlichen Anforderungen, welche durch die VDSG entstehen.

economiesuisse

Frau Bundesrätin
Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
jonas.amstutz@bj.admin.ch

14. Oktober 2021

Stellungnahme zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Im Juni 2021 haben Sie uns eingeladen, in oben genannter Sache Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. economiesuisse nimmt gestützt auf den Input der betroffenen Mitglieder aus einer übergeordneten, gesamtwirtschaftlichen Sicht wie folgt Stellung.

Zusammenfassung

Die Wirtschaft setzt sich für einen modernen und zweckmässigen Datenschutz ein, der die Innovationskraft unseres Standorts nicht behindert. Ein administrativ tragbares Vorgehen, eingebettet in die internationalen Entwicklungen ist dabei zentral. Bei der parlamentarischen Beratung zum revidierten Datenschutzgesetz ist es in wesentlichen Punkten gelungen, das Gesetz ohne verkomplizierende Schweizer Besonderheiten international abgestimmt zu verabschieden.

Der Entwurf der totalrevidierten Verordnung zum DSG (E-VDSG) folgt der vom Parlament im revDSG vorgegebenen Stossrichtung nicht. Er verschärft wesentliche Punkte des Gesetzes ohne Grund, ist inhaltlich nicht ausreichend präzise und gleichzeitig unnötig restriktiv. Statt das revDSG im Sinne von Ausführungsvorschriften zu konkretisieren, sieht die Verordnung eine Reihe von bürokratischen Zusatzvorschriften mit vielen Swiss Finishes vor, die keine Grundlage im Gesetz finden.

Die Verordnung wirkt wie ein unabhängig vom revDSG entstandenes Regelwerk. Die politischen Diskussionen und Erwägungen der DSG-Debatte wurden nicht ausreichend berücksichtigt. Dieses Problem zeigt sich sowohl in der Verordnung wie auch im Erläuterungsbericht. Der Entwurf muss unter Berücksichtigung des revDSG und insbesondere der politisch intensiv geführten Diskussion, welche zu

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

zahlreichen und wichtigen Kompromissen im Parlament geführt hat, nochmals stark überarbeitet und verbessert werden. Der vorliegende Entwurf wird von der Wirtschaft geschlossen und klar abgelehnt. Er stellt keine Grundlage für einen zweckmässigen, zukunftsgerichteten Datenschutz dar.

Gestützt auf diese Ausgangslage stellen wir den folgenden Antrag zur Revisionsvorlage:

Ausführliche Überarbeitung des Entwurfes und Respektierung der Kohärenz zum revDSG
und eine Verhinderung von Swiss Finishes und unnötiger Restriktionen; damit allfällige Verzögerungen die Aufrechterhaltung der Äquivalenz zur DSVGO nicht beeinflussen, muss diese wichtige Überarbeitung unter Einsetzung der notwendigen Ressourcen möglichst zeitnah erfolgen.

Die (nicht abschliessenden) Hauptanliegen der Wirtschaft bei einer Überarbeitung des Entwurfes:

1) Dem langwierigen politischen Prozess zum revDSG muss Rechnung getragen werden. Das Gesetz ist ein bis in die Einigungskonferenz der Räte intensiv diskutierter Kompromiss. Regeln, welche es nicht ins DSG geschafft haben, dürfen nicht über die VDSG in die Praxis einfliessen.
2) Sämtliche Swiss Finishes, welche nicht im revDSG geregelt sind und über das Niveau der DSGVO hinausgehen, widersprechen der expliziten Zielsetzung des Gesetzgebers, Kompatibilität mit der DSGVO zu erschaffen. Diese sind ersatzlos zu streichen.
3) Widersprüche zum revDSG müssen zwingend behoben werden.
4) Bei der VDSG handelt es sich um eine Ausführungsverordnung, welche nicht über die blosse Konkretisierung des Gesetzes hinausgehen darf. Zahlreiche vorgeschlagene Regelungen setzen sich mit zu weitgehenden oder gesetzlich nicht vorgesehenen Vorschriften in Widerspruch zur übergeordneten, bewusst und konsequent prinzipien- und risikobasierten gesetzlichen Ordnung und produzieren damit in der Umsetzungspraxis sehr viel zusätzlichen und unnötigen Aufwand.

Wir gliedern unsere diesbezüglichen Ausführungen dabei wie folgt:

- Unter Ziff. 1 erläutern wir die Gründe für unseren Antrag;
- Unter Ziff. 2 legen wir unsere wichtigsten Anliegen dar;
- Im Anhang finden Sie die detailliert ausformulierten Anpassungsvorschläge der Wirtschaft.

1 Ausführliche Überarbeitung des Entwurfes

In einer zunehmend digitalisierten Wirtschaft ist es von grundsätzlicher Bedeutung, dass die Datenschutzgesetzgebung eine die Innovationskraft des Standortes Schweiz nicht beeinträchtigende Balance zwischen einem angemessenen Schutz der Daten und der wirtschaftlichen Nutzung von Daten findet. Mit dem revDSG konnte im Herbst 2020 ein modernes Gesetz geschaffen werden, welches das Schutzniveau der DSGVO übernimmt, die Anliegen der Politik und Wirtschaft angemessen berücksichtigt und dadurch zahlreiche Verbesserungen gegenüber dem bisherigen DSG beinhaltet. Gerade auch durch seine Angleichung an die DSGVO wird das neue DSG für die Schweizer Unternehmen gut umsetzbar und reduziert das Problem zweier Standards.

In der Diskussion um das DSG war der EU-Angemessenheitsentscheid einer der grossen Treiber der Revision. Die Abstimmung mit der DSGVO war ein komplexes Unterfangen, denn das Gesetz musste intelligente und praktikable Ansätze finden, welche den Besonderheiten des alten DSG Rechnung trugen, die Interessen der Nutzer aufgreifen, die Wirtschaft nicht übermässig belasten und mit dem System der EU gleichwertig sind. Dabei konnte grösstenteils auf Swiss Finishes verzichtet werden. Die

Wirtschaft hat insbesondere mit Blick auf die Äquivalenz zum EU-Recht die Vorlage nach dem Prinzip «so viel wie nötig, so wenig wie möglich» begleitet. Das gleiche Prinzip hätte auch auf die VDSG angewendet werden müssen. Die grosse Menge an Swiss Finishes, die ihren Weg nun in den E-VDSG gefunden haben, führen zu einem enormen Mehraufwand für die Schweizer Wirtschaft und sind weder zweckmässig noch notwendig.

Zudem wurde der politische Prozess bei der Erarbeitung des E-VDSG nicht ausreichend berücksichtigt. So wurden Regelungen, welche im politischen Prozess um die DSG-Revision im Parlament abgelehnt worden waren, in der E-VDSG wiederbelebt (Art. 16 E-VDSG). Zwar ist der Bundesrat berechtigt, Gesetze durch Verordnungen näher auszuführen (Art. 182 Abs. 2 BV); dabei darf er aber nur «Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher ausführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beitragen» (BGE 141 II 169). Mehrere Regelungen im E-VDSG haben diesen Rahmen klar gesprengt, indem sie einen mit den Bestimmungen im revDSG vergleichbaren Regelungsgehalt aufweisen (z.B. Art. 4, Art. 15 und Art. 16). Es ist nicht nachvollziehbar, wie es dazu kommen konnte. Es ist nicht Aufgabe der Verwaltung, ein parlamentarisches Gesetz nach Abschluss des Gesetzgebungsprozesses auf dem Verordnungsweg zu verschärfen oder zu ergänzen.

All dies ist mit Blick auf die von KMU geprägte Struktur der schweizerischen Wirtschaft umso gravierender. Schon die umfassenden Regelungen im revDSG dürften für die grosse Mehrheit der KMU aus verschiedenen Gründen nur sehr schwer umsetzbar sein. Das gilt erst recht für die verschärften Regeln des E-VDSG. Viele der Vorschriften lassen sich wohl gar nicht (Art. 2 EVDSG) oder nur mit unverhältnismässigem Aufwand umsetzen. Diese Ausgangslage ist gerade deshalb besorgniserregend, weil viele der Pflichten mit strafrechtlichen Sanktionen (Art. 60ff. revDSG) bedroht sind.

Eine vernünftige Umsetzung der Datenschutzgesetzgebung ist auch für die digitale Wirtschaft und damit für die Zukunftsfähigkeit und Innovationskraft des Wirtschaftsstandorts Schweiz erforderlich. Der Bund fördert Digitalisierung umfassend und auf allen Stufen. Folgerichtig muss er das nicht zuletzt auch beim Thema Datenschutz tun.

Aus diesen Gründen müssen der E-VDSG und der Erläuterungsbericht unter Berücksichtigung der hier aufgebrachten Kritikpunkte überarbeitet werden. Dabei sollte auch an dem sonst verbreiteten Gebrauch festgehalten werden, dass sich jeweils neben dem Artikel einer Verordnung ein Verweis zum korrespondierenden Gesetzesartikel findet.

2 Die Hauptanliegen der Wirtschaft bei einer Überarbeitung des Entwurfes

Die wichtigsten Kritikpunkte aus Sicht der Wirtschaft sind dabei die Folgenden:

1) Artikel und Prinzipien, welche im politischen Prozess zum DSG abgelehnt und aus dem Entwurf zum revDSG gestrichen wurden, sollten nun nicht durch die VDSG wieder eingeführt werden. So z.B. Art. 16, der eine Informationspflicht einführen möchte, von der man sich im Vernehmlassungsprozess zum revDSG verabschiedet hatte.

2) Zahlreiche Swiss Finishes führen zu zwei Standards für die Schweiz. Die folgenden Artikel sind dabei besonders gravierend und müssen entweder gestrichen oder dahingehend geändert werden, dass sie keine zusätzlichen, über die DSGVO hinausgehenden Pflichten beinhalten:
    a. Art. 4 E-VDSG
    b. Art. 13 Abs. 1 E-VDSG
    c. Art. 15 E-VDSG
    d. Art. 19 E-VDSG

3) Widersprüche wie in Art. 13 E-VDSG müssen unbedingt behoben werden. Der Artikel kreiert eine Inkonsistenz in Bezug auf Art. 19 revDSG, Art. 13f. DSGVO und auch zum bisherigen Gesetz (Art. 14 DSG).

4) Betreffend die Inkraftsetzung sollte des immensen Aufwandes, der auf die KMU, aber auch die grösseren Unternehmen zukommt, durch eine **angemessene Umsetzungsfrist** bedacht werden. Nach Rückmeldung unserer Mitglieder erachten wir einen Zeitraum von mindestens einem Jahr laufend ab Feststehen/Veröffentlichung der definitiven Fassung der Verordnung als notwendig und angebracht.

5) Weitere zentrale Änderungsvorschläge der Wirtschaft beziehen sich auf:
   a. Art. 3 E-VDSG
   b. Art. 8 E-VDSG
   c. Art. 16 E-VDSG

Im Anhang finden Sie konkrete und im Detail ausgearbeitete Anpassungsvorschläge der Wirtschaft. Damit lassen sich die obstehenden Kritikpunkte angehen. Wir sind gerne bereit, Sie bei den von uns vorgeschlagenen und dringend notwendigen Anpassungen zu unterstützen. Vielen Dank für die Berücksichtigung unserer Anliegen. Bei Fragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse

Erich Herzog
Mitglied der Geschäftsleitung

Leonie Ritscher
Wissenschaftliche Mitarbeiterin Wettbewerb & Regulatorisches

Anhang: Anpassungsvorschläge der Wirtschaft für die VDSG

Anhang: Anpassungsvorschläge der Wirtschaft für die VDSG

Anliegen, sofern auf Basis des bisherigen Entwurfes weitergearbeitet wird

1. Kapitel: Allgemeine Bestimmungen

Artikel 1 (Grundsätze)

Antrag economiesuisse:

1) Sachlogische Anpassung beim Begriff des «Risikos».
2) Berücksichtigung des Implementierungsaufwands statt der -kosten als Kriterium aufnehmen.
3) Anerkennung eines Umsetzungsermessens des Verantwortlichen.

Begründung:

1) Ein Risiko ergibt sich sachlogisch vorab aus einer potenziellen Verletzung der Datensicherheit für die betroffene Person. Für den Fall des Vorliegens einer solchen potenziellen Verletzung stellt sich nachgelagert die Frage nach der Eintrittswahrscheinlichkeit. Dabei sind die Anforderungen an die Datensicherheit höher, je grösser die Eintrittswahrscheinlichkeit ist. Ohne potenzielle Datensicherheitsverletzung stellt sich umgekehrt die Frage nach der Eintrittswahrscheinlichkeit gar nicht. Die Formulierung in Art. 1 Abs. 1 lit. b E-VDSG ist verwirrend, weil sie diese sachlogisch zwingende Reihenfolge nicht beachtet. Die Formulierung in lit. b ist deshalb richtigerweise umzudrehen.
2) Die Aufführung der Implementierungskosten als Kriterium zur Beurteilung der Angemessenheit von technischen oder organisatorischen Massnahmen (sog. TOM) zur Gewährleistung der Datensicherheit ist nicht ausreichend. Neben eigentlichen Implementierungskosten fallen typischerweise auch weitere Aufwendungen an, welche zu berücksichtigen sind - so etwa personelle, zeitliche und organisatorische Aufwendungen. Innerhalb einer Auswahl gleichwertiger angemessener Massnahmen darf der Verantwortliche die kostengünstigere auswählen. Dies ist selbstverständlich, da es sich bereits aus dem allgemeinen Verhältnismässigkeitsprinzip ergibt, wird sinnvollerweise aber dennoch erwähnt.
   Zudem sollte nicht allein auf die Implementierungskosten, sondern generell auf den Implementierungsaufwand, der etwa aus personellen, zeitlichen und organisatorischen Aufwendungen besteht, abgestellt werden.
3) Ob, wann und wie eine Überprüfung der TOM stattfinden soll, muss durch den Verantwortlichen bzw. den Auftragsbearbeiter selbst entschieden werden. Nur er ist in der Lage, den Besonderheiten des Einzelfalls hinreichend Rechnung zu tragen. Ist die Gefährdung der Rechte von Betroffenen grösser, so ist der zeitliche Abstand bis zur nächsten Prüfung sachlogisch kürzer. Die einseitige Fokussierung auf den zeitlichen Abstand einer Prüfung und die zwingende Verknüpfung einer Prüfpflicht sind somit nicht sachgerecht, unnötig einengend und stehen im Widerspruch zum risikobasierten Ansatz. Der Begriff «angemessene Abstände» ist durch «angemessene Weise» zu ersetzen.

Formulierungsvorschlag:
1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:
a. […];

b. die verbleibenden ~~Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren~~ potenziellen Auswirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit;
c. […];
d. Implementierungs~~kosten~~*aufwand*.
2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen~~r~~ ~~Abständen~~ Weise zu überprüfen.

Artikel 2 (Schutzziele)

Antrag economiesuisse:
Der Verordnungstext bringt zu wenig klar zum Ausdruck, dass sich die Notwendigkeit der in Art. 2 E-VDSG aufgeführten Schutzziele nach den in Art. 1 E-VDSG vorgeschriebenen Grundsätzen richtet.

Begründung:
Die in Art. 2 Abs. 2 E-VDSG aufgeführten Schutzziele sind veraltet, zu absolut und zu detailliert geregelt. Entsprechend ihrer abstrakten Formulierung erwecken die Schutzziele zudem fälschlicherweise den Eindruck, dass es sich um absolut zu erreichende Anforderungen handelt. Insofern werden statt Minimalanforderungen fälschlicherweise Maximalanforderungen formuliert.
Im Kern muss es im - hier zu regelnden - Bereich der Datensicherheit um die Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit gehen. Eine generelle Dokumentationspflicht ist schon deshalb abzulehnen, weil diese so auch vom Gesetzgeber ausdrücklich abgelehnt worden ist.
Selbst die tatsächlich aufzuführenden Schutzziele Verfügbarkeit, Integrität, Verfügbarkeit und Belastbarkeit haben nur beispielhaften Charakter. Sie müssen namentlich dann nicht umgesetzt werden, wenn die Analyse nach Art. 1 E-VDSG dies nicht gebietet. Die Formulierung in der Verordnung sollte dies deutlich zum Ausdruck bringen. Damit sollen nicht zuletzt auch KMU vor unnötigem administrativem Aufwand bewahrt werden. Die vorgeschlagenen Formulierungen bringen zum Ausdruck, dass die Aufzählung in Art. 2 E-VDSG weder vollständig noch verpflichtend ist. Umgesetzt werden muss nur das, was nach Art. 1 E-VDSG zur Gewährleistung einer angemessenen Datensicherheit notwendig ist. Um dieses Ziel zu erreichen, können jedoch auch Massnahmen zur Anwendung kommen, die in Art. 2 E-VDSG nicht erwähnt sind. Mit den von uns beantragten Anpassungen ist die Liste auch konform mit den Anforderungen von Art. 32 EU-DSGVO. Ohne entsprechende Anpassungen läge demgegenüber ein kontraproduktiver "Swiss Finish" vor, welcher wegen unnötigen Zusatzaufwendungen und Zusatzrisiken auch die EU-Äquivalenz gefährden würde.

Formulierungsvorschlag
~~Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen~~ Basierend auf den Grundsätzen nach Art. 1 ist insbesondere zu beurteilen, welche der nachfolgenden Schutzziele für Systeme und Dienste in Zusammenhang mit der Bearbeitung von Personendaten in Anwendung des risikobasierten Ansatzes im konkreten Fall anwendbar sind:
a. Vertraulichkeit
b. Integrität
c. Verfügbarkeit
d. Belastbarkeit

Artikel 3 (Protokollierung)

Antrag economiesuisse:
Ersatzlos streichen

Begründung:
Diese Bestimmung ist in mehrfacher Hinsicht problematisch. Das Parlament hat trotz detaillierter Formulierung der Anforderungen an die Datenschutzfolgenabschätzungen in Art. 22 revDSG bewusst auf eine Protokollierungspflicht verzichtet. Darüber hinaus ergibt sich aus zahlreichen Voten im Parlament ebenso wie auch aus der finalen Fassung des revDSG mit aller wünschbaren Deutlichkeit, dass das Parlament am - auch ausserhalb des Datenschutzrechts - bewährten prinzipien- und risikobasierten Regulierungsansatz festhalten wollte und – nicht zuletzt, um unnötigen Aufwand für die zahlreichen KMU zu verhindern – namentlich auf unnötige Formvorschriften verzichten wollte. Dazu gehören neben strikte formulierten Dokumentations- und Protokollierungspflichten u.a. auch strikte Aufbewahrungsfristen (deren Dauer über die E-VDSG verteilt uneiheitlich und wohl eher zufällig mal kürzer, mal länger geregelt werden). Die Festlegung der geeigneten organisatorischen und technischen Massnahmen (TOM) zur Umsetzung von Pflichten gemäss revDSG muss in Anwendung des im revDSG – wie bisher – bewusst gewählten prinzipien- und risikobasierten Ansatzes jedem Verantwortlichen bzw. Auftragsbearbeiter nach vernünftigem Ermessen obliegen, namentlich entsprechend den Kriterien Grösse, Struktur, Komplexität, Risiken und Geschäftsmodell (vgl. schon oben Ziff. A. 1-7). Nach alledem widerspricht die in Art. 3 E-VDSG vorgeschlagene Protokollierungspflicht dem klaren gesetzgeberischen Willen, hat entsprechend keine gesetzliche Grundlage und wäre überdies auch in seinen Wirkungen kontraproduktiv, würden doch in Anwendung dieser Pflicht umfassende Protokolle bzw. Logs über praktisch sämtliche Personendatenflüsse eines Verantwortlichen erstellt. Eine solche Pflicht auf Stufe E-VDSG wäre eine klare Verletzung des im revDSG verankerten Verhältnismässigkeitsprinzips (vgl. namentlich Art. 6 Abs. 2 u. 3 revDSG), mithin dem wohl wichtigsten Grundprinzip für ein funktionierendes Datenschutzsystem. In Anwendung von Art. 3 E-VDSG würden denn auch statt Datenschutzprobleme zu lösen widersinnigerweise neue geschaffen. Zuletzt müsste auch der Auftragsbearbeiter protokollieren, der aber u.U. gar nicht weiss, ob eine Folgeabschätzung durchgeführt wurde und was ihr Ergebnis war.

Nach alledem ist Art. 3 E-VDSG konsequenterweise ersatzlos zu streichen.

Eventualiter:
Will man wider Erwarten nicht so weit gehen, müsste nach dem Gesagten im Titel und in den Absätzen 1-3 zumindest die Anforderung "Protokollierung" durch "angemessene Dokumentation" ersetzt werden, sowie in Abs. 4 "Protokolle mindestens 2 Jahre aufzubewahren" durch: "Die Aufbewahrungsfrist muss, sofern eine solche gesetzlich festgelegt ist, abhängig von Dauer und Datenbearbeitung und generell angemessen sein".

Artikel 4 (Bearbeitungsreglement von privaten Personen)

Antrag economiesuisse:
Ersatzlos streichen

Begründung:
Die Regelung wurde im Wesentlichen aus Art. 11 der geltenden VDSG übernommen. Schon jene Bestimmung blieb aber insofern «toter Buchstabe», als es ein solches «Bearbeitungsreglement» in dieser Form in der operativen Praxis von Unternehmen nicht gibt. Vielmehr werden die zahlreichen notwendigen Regelungen gemäss bewährter Usanz in einem ganzen Paket von sich gegenseitig ergänzenden

Weisungen samt dazugehörigen Prozessen und Listen mit Aufgaben, Kompetenzträgern und Verantwortlichkeiten abgebildet. Diese sind sehr viel wirkungsvoller als ein starres Reglement. Das in der E-VDSG vorgesehene Bearbeitungsreglement kann die immer komplexeren Datenbearbeitungen in der Praxis nicht mehr sinnvoll abbilden. Diese Aufgabe übernimmt zu Recht das neu zu führende Verzeichnis der Bearbeitungstätigkeiten (Art. 12 revDSG).

Umso unverständlicher ist, dass die Regelung von Art. 4 E-VDSG weitgehend deckungsgleich mit den Anforderungen an das gemäss Art. 12 revDSG zu erstellende Verzeichnis der Bearbeitungstätigkeiten ist, was unnötigerweise Rechtsunsicherheit und unnötigen Doppelaufwand produziert. Das revDSG sieht in Art. 12 bereits vor, dass die Datenverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten führen müssen. Dieses muss ähnliche Informationen enthalten wie das Bearbeitungsreglement. Mit der Einführung des Verzeichnisses macht ein zusätzliches Bearbeitungsreglement keinen Sinn, zumal dieses weitgehend die gleichen Informationen enthält.

Die Aufgreifkriterien gemäss Art. 4 Abs. 1 E-VDSG sind keineswegs klar abgrenzbar. Im Bereich Profiling besteht unter Würdigung sämtlicher Kriterien ein gewisses Ermessen, wann die Grenze zu "hohem Risiko" erreicht ist. Die gesetzliche Regelung (vgl. Art. 5 lit. f und g revDSG) gibt hierzu auch keine klaren Vorgaben, weil nur technische Beschreibungen ohne echte Abgrenzungskriterien festgelegt wurden. Namentlich wiederholt die Regelung für Profiling mit hohem Risiko (Art. 5 lit. g revDSG) im Kern einen technischen Beschrieb, welcher auf jedes Profiling zutrifft und lässt offen, wann die Grenze zu einem "hohen Risiko" erreicht ist. Kritisch ist auch das Aufgreifkriterium "Bearbeitung umfangreicher besonders schützenswerter Personendaten" gemäss Art. 4 Abs. 2 Abs. 1 lit. b E-VDSG. Dies dürfte bei HR-Daten relativ rasch der Fall sein, auch bei KMU. Die offene Formulierung "umfangreich" ist deshalb als Aufgreifkriterium nicht geeignet. Nach alledem müssten sorgfältige Verantwortliche im Zweifelsfall einen Grossteil ihrer Datenbearbeitungen den Regeln von Art. 4 E-VDSG unterstellen. Gemäss Systematik von Art. 4 Abs. 1 E-VDSG ist dies aber gar nicht beabsichtigt, soll doch Art. 4 E-VDSG nur auf Ausnahmen von der Regel anwendbar sein. Diese gänzlich misslungene Regelung ist ein eigenständiger Grund für die ersatzlose Streichung von Art. 4 E-VDSG.

Auch hat ein Bearbeitungsreglement mit der Datensicherheit im eigentlichen Sinne, die Art. 8 Abs. 3 revDSG regelt, nichts zu tun. Es fehlt daher die gesetzliche Grundlage für eine Pflicht, ein Bearbeitungsreglement zu führen.

Art. 4 E-VDSG generiert somit statt Klärung bloss Verwirrung und unnötige Abgrenzungsprobleme. Zwei weitgehend deckungsgleiche Regelungen zu erlassen, ist gänzlich sinnlos. Dies umso mehr, als die meisten Schweizer Unternehmen überdies auch grenzüberschreitende Geschäfte betreiben und deshalb entsprechende Verzeichnisse nicht nur nach dem revDSG, sondern überdies auch nach der EU-DSGVO erarbeiten müssen.

Demzufolge ist Art. 4 E-VDSG ersatzlos zu streichen.

Artikel 6 (Modalitäten)

Antrag economiesuisse

1) Klarstellung im Erläuterungsbericht, dass die VDSG – anders als die DSGVO – keinen Mindestinhalt an den ADV vorschreibt.
2) Streichung von Abs. 1
3) Streichung von Abs. 2

Begründung:

1) Es ist unklar, was die Ausführungen auf S. 24 der Erläuterungen zu den Anforderungen an den Inhalt des ADV gemäss Art. 22 Abs. 3 DSGVO bezwecken, zumal diese in Art. 6 E-VDSG nicht vorgesehen sind. Diese Ausführungen suggerieren, dass der ADV gemäss Art. 6 VDSG den inhaltlichen Anforderungen der DSGVO genügen müsse. Hierfür findet sich indes keine gesetzliche Grundlage. Auch die E-VDSG enthält keine inhaltlichen Vorgaben.
2) Absatz 1 wiederholt zuerst eine Banalität und ist gleichzeitig ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall eingeschränkt ist, auch dann, wenn ihm nichts vorgeworfen werden kann. Dem sollte nicht so sein. Es ist ohnehin nicht klar, was mit «für den Datenschutz verantwortlich» gemeint ist. Strafrechtliche Verantwortlichkeit kann es nicht sein, und aufsichtsrechtliche Verantwortlichkeit setzt ebenfalls Kontrollmöglichkeiten voraus. Wird die Verantwortlichkeit schliesslich als zivilrechtliche Haftung verstanden, dann wird mit dieser Regelung eine vom Gesetzgeber nicht vorgesehene Kausalhaftung eingeführt. Hierfür fehlt klarerweise eine gesetzliche Grundlage. Dies würde auch über Art. 82 Abs. 3 DSGVO hinausgehen. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR. Zudem ist die Formulierung «sicherstellen» inhaltlich falsch. Der Verantwortliche kann nur «dafür Sorge tragen».
   Auch der zweite Satz ist mangelhaft, da ihm ebenfalls eine gesetzliche Grundlage fehlt. Nach Art. 9 Abs. 1 lit. a revDSG hat der Verantwortliche dafür zu sorgen, dass die Daten so bearbeitet werden, wie er es selbst darf. Nach Satz 2 hat er jedoch auch für die Durchsetzung seines eigenen Vertrags zu sorgen, selbst wenn dieser strenger sein sollte als das Gesetz. Macht er also einen zu strengen Vertrag, erlaubt aber seinem Auftragsbearbeiter eine Bearbeitung, die noch dem Gesetz entspricht, ist diese Vorschrift bereits verletzt. Die Regel verwirrt also mehr als sie nutzt. Schon nach Art. 9 Abs. 1 lit. a revDSG hat der Verantwortliche dafür zu sorgen, dass das DSG eingehalten wird. Das sollte genug Schutz bieten, sodass die Regelung hier obsolet wird.
3) Der Sinn und Zweck der Regelung von Abs. 2 erschliesst sich nicht, da der Regelungsgehalt bereits durch die Art. 16 und 17 revDSG (Bekanntgabe von Personendaten ins Ausland) abgedeckt ist. Gemäss Erläuterungsbericht entspricht der neue Art. 6 Abs. 2 E-VDSG dem geltenden Art. 22 Abs. 3 VDSG. Dabei handelt es sich aber um eine Bestimmung für Bundesorgane, während Art. 6 Abs. 2 E-VDSG sowohl für Datenbearbeitungen Privater als auch für solche von Bundesorganen gelten soll. Aus dem Erläuterungsbericht geht nicht hervor, warum diese Bestimmung nun auch für Private gelten soll.
   Offen bleibt auch, weshalb es die Regelung überhaupt braucht bzw. auf welche Rechtsgrundlage sie sich stützt.
   Die Regelung würde nur dort halbwegs Sinn machen, wo ein Schweizer Verantwortlicher einen ausländischen Auftragsbearbeiter einsetzt, um Daten zu bearbeiten, ohne dass es zu einer Bekanntgabe aus der Schweiz kommt und somit Art. 16 revDSG nicht greift. Systematisch wäre aber auch dieser Fall in Art. 16 revDSG zu regeln und nicht in der VDSG. Zudem ist diese Konstellation ein absoluter Sonderfall. Eine eigene Regelung in der E-VDSG rechtfechtfertigt sich somit nicht. Die Regelung ergibt sich im Übrigen ohnehin bereits aus Art. 9 Abs. 1 lit. a revDSG, und zwar systematisch korrekt, während sie hier systematisch falsch angelegt ist: Im Falle einer Auftragsbearbeitung geht es nicht um die Sicherstellung eines gleichwertigen Datenschutzes, da der Auftragsbearbeiter die Daten gar nicht in eigener Regie bearbeiten darf. Vielmehr geht es darum sicherzustellen, dass die Daten nur so bearbeitet werden, wie der Verantwortliche dies darf – und so steht es schon in Art. 9 Abs. 1 lit. a revDSG.

Aufgrund obiger Ausführungen sind Art. 6 Abs. 1 sowie Abs. 2 E-VDSG ersatzlos zu streichen.

Artikel 8 (Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs)

Antrag economiesuisse:
Sowohl in Abs. 1 als auch in Abs. 6 braucht es eine Anpassung, um klarzustellen, dass sich die Regelung nur an den Bundesrat richtet.

Begründung:
Nach Art. 16 Abs. 1 revDSG legt nunmehr der Bundesrat fest, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten.
Der Wortlaut von Art. 8 Abs. 1 und 6 E-VDSG kann dahingehend missverstanden werden, dass die verantwortliche Stelle – und nicht der Bundesrat – die Angemessenheit des Datenschutzes in einem Empfängerstaat feststellen muss. Somit muss klargestellt werden:

- dass sich dieser Artikel **nur an den Bundesrat (BR) richtet**;
- dass der **BR einzige kompetente Stelle wird, welche eine solche Positiv-Liste erlassen kann** – der EDÖB wird vom BR konsultiert, kann jedoch keine eigene Liste herausgeben. Die Aufgabe des EDÖB liegt neu lediglich darin, Empfehlungen/Assessmentvorgaben für den Datentransfer in Länder zu formulieren, die nicht auf der Positiv-Liste sind;
- dass die Positiv-Liste des BR **verbindlich ist**.

Formulierungsvorschlag:
1 Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen~~t werden~~: (…)

6 Der Bundesrat konsultiert den EDÖB ~~wird~~ vor jedem Entscheid über die Angemessenheit des Datenschutzes ~~konsultiert.~~

Implikationen als Folge der Rechtsprechung des Europäischen Gerichtshofs (EuGH) in der Rechtssache Schrems II sowie des **Positionspapiers** und der **Handlungsanleitung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in gleicher Sache (Art. 8 Abs. 1 Satz 2 E-VDSG und Abs. 7 E-VDSG)**

Wie bereits erwähnt, legt nunmehr der Bundesrat fest, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten. Gemäss dem Erläuternden Bericht des Bundesamtes für Justiz soll daher die Verordnung neu die Kriterien regeln, welche der Bundesrat bei seinem Entscheid berücksichtigt. In Anhang 1 sind tabellarisch diejenigen Staaten und internationalen Organe aufgeführt, welche über ein angemessenes Datenschutzniveau verfügen.
Der Bundesrat erstellt die Liste der Länder mit angemessenem Datenschutz nach bestem Wissen und Gewissen. Die Verantwortlichen dürfen sich zwar im Prinzip auf diese Liste verlassen und müssen mithin nicht per se eigene Abklärungen vornehmen, welche die Einschätzung des Bundesrates bestätigen. Die Liste geniesst aber keinen öffentlichen Glauben (anders als z.B. das Grundbuch). Die Verantwortlichen dürfen sich deshalb nur, aber immerhin solange auf Gutgläubigkeit berufen und sich auf die Liste verlassen, wie ihnen aus eigener Erfahrung nichts Gegenteiliges bekannt ist. Ohne dahingehenden eigenständigen Verdachtsanlass selbst Abklärungen über die Richtigkeit der Liste vornehmen muss der Verantwortliche aber nicht (vgl. schon BJ-Erläuterungen zum DSG vom 24. März 2006, S. 8, Antwort zu Frage 49).

Am 18. Juni 2021 hat der EDÖB eine Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug veröffentlicht. Soweit danach ein Land auf der Staatenliste (des EDÖB und künftig des Bundesrates) fehlt oder mit einem ungenügenden Schutzniveau ausgewiesen ist, muss der Datenexporteur prüfen, ob kumulativ folgende vier Garantien eingehalten werden:

- klare Rechtsgrundlage betreffend Zwecke sowie Verfahren und materiellrechtliche Voraussetzungen des behördlichen Datenzugriffs und Befugnisse der Behörden;
- Verhältnismässigkeit der behördlichen Befugnisse und Massnahmen;
- wirksame gesetzlich verankerte Rechtsbehelfe für die Durchsetzung von Rechten von Betroffenen in der Schweiz;
- Rechtsweggarantie und Zugang zu einem unabhängigen und unparteiischen Gericht.

Erfüllt das lokale Recht die genannten Garantien nicht, muss der Datenexporteur weitere technische, organisatorische und rechtliche Massahmen treffen. Kann durch solche Massnahmen der fehlende Schutz nicht ausgeglichen werden, folgt daraus, dass die Datenbekanntgabe ins Ausland ausgesetzt bzw. beendet wird.
Nach der Handlungsanleitung des EDÖB soll der Datenexporteur als gutgläubig gemäss Art. 3 Abs. 1 ZGB gelten, soweit er Daten in einen Staat übermittelt, der auf der Staatenliste als ein solcher mit angemessenem Datenschutzniveau aufgeführt wird. Hierbei soll es sich allerdings um eine widerlegbare Vermutung handeln. So soll der verantwortliche Datenexporteur bei der Erfassung und Analyse des Datentransfers alle nötigen Abklärungen vornehmen müssen, wie z.B. Einholen von unabhängigen Rechtsgutachten, u.a. zu folgenden Aspekten:

- Geltende Rechtsvorschriften im Zielland;
- Praxis der Verwaltungsbehörden und Gerichtsbehörden;
- Rechtsprechung.

Verbindlichkeit des Entscheids des Bundesrats zur Angemessenheit des Datenschutzes (Klarstellung in Art. 8 Abs. 1 Satz 2 E-VDSG)

Die durch den EDÖB vorgeschlagene Prüfung der obenstehenden Garantien durch den Datenexporteur muss sich aufgrund einer positiven Entscheidung des Bundesrats hinsichtlich der Angemessenheit des Datenschutzes in einem Drittstaat erübrigen. Dies folgt bereits daraus, dass ohne die Vorlage solcher Garantien nicht von einem angemessenen Datenschutz ausgegangen werden kann.

Eine zusätzliche Einzelfallprüfung und die damit einhergehende Beurteilung und Entscheidung zur jeweiligen (ausländischen) Rechtsordnung des Importstaates hinsichtlich hinreichender Transparenz und Rechtsschutz für die betroffenen Personen durch den Datenexporteur erscheint darüber hinaus aus Praktikabilitätsgründen weder als durchführbar noch als zielführend.

Denn einerseits sind die relevanten Rechtsgrundlagen, Rechtsprechung sowie insbesondere die Behördenpraxis für (geheime) Zugriffe nicht einheitlich kodifiziert und/oder öffentlich zugänglich. Der Bundesrat und speziell das EDA und das EJPD verfügen hier über die besten Quellen und Kenntnisse. Andererseits wäre eine solche Beurteilung als unverhältnismässig aufwändig zu werten, da diese eine Momentaufnahme widerspiegeln würde, die einem raschen Wandel unterliegen kann. Folglich könnte ein Verantwortlicher gar nicht innert vertretbarer Zeit adäquat auf Änderungen reagieren und sofortige neue Dispositionen treffen.

Darüber hinaus würde der Umstand, Unternehmen als Datenexporteure mit der Aufgabe zu betrauen, die Angemessenheit der Rechtsordnungen des Importstaates zu untersuchen und zu beurteilen, Art. 16 revDSG i.V.m. Art. 8 E-VDSG widersprechen. Diese Normen legen fest, dass die Angemessenheitsprüfung

und die damit einhergehende Entscheidung vom Bundesrat und nicht von den datenexportierenden Stellen vorgenommen werden muss. Sollten nicht einheitlich der Bundesrat, sondern die datenexportierenden Verantwortlichen solche Beurteilungen vornehmen, sind unterschiedliche Ergebnisse hinsichtlich bestimmter Länder und Datenverarbeitungen vorprogrammiert. Dies würde im Ergebnis trotz viel Aufwand keine Rechtssicherheit schaffen. Die Liste des Bundesrats verlöre dadurch jeden Sinn.

Um eine faktische Aushöhlung der Feststellungskompetenz des Bundesrates sowie unterschiedliche Ergebnisse der Bewertung und eine damit einhergehende Rechtsunsicherheit zu vermeiden, muss deshalb auf Stufe E-VDSG ausdrücklich geklärt werden, dass sich die Verantwortlichen als Datenexporteure auf den Entscheid des Bundesrates zur Angemessenheit verlassen dürfen und keine zusätzlichen Abklärungen treffen müssen.

Daher soll zur Klarstellung ein neuer Satz 2 in Art. 8 Abs. 1 E-VDSG eingefügt werden.

Formulierungsvorschlag
1) Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~ muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen~~t werden~~:
(a-e) …
Die Verantwortlichen dürfen sich auf den Entscheid des Bundesrates zur Angemessenheit des Datenschutzes nach Satz 1 verlassen und müssen keine zusätzlichen Abklärungen treffen.

Staaten oder internationale Organe ohne angemessenen Datenschutz (Klarstellung in Art. 8 Abs. 7 E-VDSG)

Alle nicht auf der Liste des Bundesrates aufgeführten Länder gelten per se als Länder mit nicht angemessenem Datenschutz. Wollen Verantwortliche in solche Länder Personendaten versenden bzw. dort bearbeiten (lassen), müssen sie selbst abklären, ob ein angemessener Datenschutz gegeben ist oder andernfalls ergänzend geeignete angemessene Zusatzmassnahmen treffen. Das Urteil Schrems II des EuGHs generiert entgegen den Leitlinien des EDÖB vom 18. Juni 2021 in diesem Zusammenhang keine zusätzliche Liste von Ländern mit besonderem Risiko. Dies schon deshalb, weil sachlogisch bei jedem Land mit nicht angemessenem Datenschutz damit zu rechnen ist, dass spezifische Behörden und Stellen wie z.B. Geheimdienste ungefragt Einsicht in die betreffenden Daten nehmen und deshalb auch vom Urteil Schrems II erfasst sind. Eine solche Liste von Ländern mit hochgradig nicht angemessenem Datenschutz dürfte auch aus politischen Gründen nicht opportun sein, da sie wichtige internationale Beziehungen der Schweiz nachhaltig gefährden könnte. Dies ist in Art. 8 E-VDSG im Sinne einer notwendigen Präzisierung klar zu stellen, um obgenannte Leitlinien des EDÖB zu entkräften, sachlogisch in einem neuen Abs. 7.

Sollte an der durch den EDÖB vorgeschlagenen zusätzlichen Prüfung der obenstehenden Garantien, welche aus einer entsprechenden Auslegung der Schrems-II-Rechtsprechung des EuGHs resultiert, festgehalten werden, müsste die Prüfung dieser Garantien sachlogisch ebenfalls einheitlich durch den Bundesrat erfolgen. Dies auch deshalb, weil die Abgrenzung zwischen "nicht angemessen" und "hochgradig nicht angemessen" zwingend Wertungen beinhaltet, welche gesamthaft einheitlich von einer kompetenten Stelle anzuwenden sind. Nur dadurch wird ein in sich stimmiges Regelungssystem für die gesamte Thematik geschaffen, welches statt Verwirrung tatsächlich Rechtssicherheit schaffen würde. Andernfalls ergäben sich kontraproduktive Widersprüche zwischen der Liste des Bundesrates und den Zusatzlisten der Verantwortlichen. Als Folge davon würde die bereits vorstehend skizzierte Rechtsicherheit (oben Ziff. 2.2) trotz viel Aufwand sogar noch weiter erhöht.

Eine Einzelfallprüfung und eine damit einhergehende Beurteilung und Entscheidung zur jeweiligen (ausländischen) Rechtsordnung des Importstaates hinsichtlich hinreichender Transparenz und Rechtsschutz für die betroffenen Personen durch den Datenexporteur erscheint aus Praktikabilitätsgründen weder als durchführbar noch als zielführend.

Nach alledem ist zur Klarstellung ein neuer Absatz 7 in Art. 8 E-VDSG einzufügen.

[…] 7) Werden Personendaten ins Ausland in einen Staat oder ein Gebiet ohne angemessenen Datenschutz bekanntgegeben, können ergänzende Massnahmen zu den Garantien gemäss Art. 16 Absatz 2 Buchstabe b und c DSG erforderlich sein, um einen geeigneten Datenschutz zu gewährleisten. Der Bundesrat stellt fest, ob ergänzende Massnahmen erforderlich sind. Die betroffenen Staaten und Gebiete sind im Anhang 1a aufgeführt. Der Entscheid des Bundesrates bezüglich der Erforderlichkeit ergänzender Massnahmen ist verbindlich.

Artikel 9 (Datenschutzklauseln und spezifische Garantien)

Antrag economiesuisse:
Zumindest Abs. 1 lit. d, e, f, h und j sollen gestrichen werden. Lit. a soll um den Grundsatz der Transparenz ergänzt und in lit. g muss der «berechtigte Empfänger» durch den «Empfänger» ersetzt werden.

Begründung:
- Die von Art. 9 E-VDSG gestellten Anforderungen sind nicht erforderlich. Der EDÖB muss sie ohnehin prüfen. Zudem erreichen sie ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Diese Anforderungen verursachen unverhältnismässig hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden.
- In den Bearbeitungsgrundsätzen (lit. a) fehlt der Grundsatz der Transparenz.
- Das Erfordernis in lit. d und e, den Namen der Staaten oder der internationalen Organisationen zu nennen, denen Personendaten bekanntgegeben werden (soweit hiermit Weiterübermittlungen gemeint sind, was nicht klar ist), hat keine rechtliche Grundlage. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Auch die EU SCC beschränken sich darauf.
- Lit. f ist bereits mit dem Grundsatz der Verhältnismässigkeit in lit. a abgedeckt, und damit redundant und zu streichen.
- Lit. g geht zu weit, indem es die «berechtigten» Empfänger verlangt. Relevant sind die «Empfänger», also normalerweise die Parteien, welche den Vertrag abschliessen und damit bereits ersichtlich sind.
- Lit. h ist klarerweise unnötig und seine Anwendung wäre unverhältnismässig aufwendig. Andere bestehende Bestimmungen genügen, um die Garantien zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.
- In Abs. 2 sollte die Datenschutzklausel die Pflicht des Empfängers enthalten, die betroffenen Personen zu informieren. Es ist nicht Aufgabe des Auftragsverarbeiters, die betroffenen Personen zu informieren; dies ist Aufgabe des Verantwortlichen.

Aus diesen Ausführungen folgt überdies, dass der Anforderungskatalog in Art. 9 Abs. 1 E-VDSG entweder anzupassen ist, um unterschiedliche Konstellationen abzudecken (Verantwortlicher, Auftragsbearbeiter) und das Wort «mindestens» durch «je nach den Umständen» zu ersetzen ist.

Das DSG schreibt – wie die DSGVO – kein proaktives „Sicherstellen“ der Einhaltung der Garantien durch den Verantwortlichen vor. Ein Eingreifen in Fällen, in welchen ein solches „Nicht-Einhalten“ und damit eine Verletzung der Vertragspflichten eintritt, ist jedoch eine Reaktion durch den Verantwortlichen selbstverständlich, und kann entsprechend auch in Art. 9 Abs. 2 in die Verordnung aufgenommen werden.

Demnach ist Art. 9 E-VDSG wie folgt anzupassen:

Formulierungsvorschlag:

1) Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen ~~mindestens~~ je nach den Umständen ~~die~~ folgende~~n~~ Punkte regeln:
    a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung, ~~und~~ der Richtigkeit und der Transparenz;
    b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen;
    c. die Art und den Zweck der Bekanntgabe von Personendaten
    d. ~~die Namen der Staaten, in die Personendaten bekanntgegeben werden;~~
    e. ~~die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden;~~
    f. ~~die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;~~
    g. die Modalitäten der Weitergabe ~~zur Bearbeitung der~~ von Daten ~~berechtigten~~ an Empfängerinnen und Empfänger;
    h. ~~die Massnahmen zur Gewährleistung der Datensicherheit;~~
    i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;
    j. ~~die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren;~~
    k. […]
2) Der Verantwortliche muss angemessene Massnahmen treffen, ~~um sicherzustellen~~wenn~~dass~~ die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien nicht einhält.

3) Wurde der EDÖB über die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die:
    a. unter denselben Datenschutzklauseln oder Garantien erfolgen, soweit die Kategorien der Empfängerinnen und Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder
    b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen Unternehmen, die zum selben Konzern gehören, stattfinden, soweit die Datenschutzklauseln oder Garantien weiterhin einen geeigneten Datenschutz gewährleisten.

Artikel 10 (Standarddatenschutzklauseln)

Antrag economiesuisse:
Der Empfänger kann nicht verpflichtet werden, „die schweizerischen Datenschutzvorschriften" einzuhalten. Das ist im Erläuterungsbericht klarzustellen.
Und
Ersetzen des Begriffs „Sicherstellung" durch „darauf hinwirken".
Und
Präzisierung, dass sich die Angemessenheit der geforderten Massnahmen nach den Umständen im konkreten Einzelfall richte und die Anforderungen insb. dann höher seien, wenn es sich um besonders schützenswerte Personendaten handle.

Begründung:
Im Erläuterungsbericht (S. 28) ist festgehalten, dass der Empfänger verpflichtet werden müsse, „die schweizerischen Datenschutzvorschriften" einzuhalten.

Das ist unzutreffend; er muss die Standardklauseln einhalten, nicht jedoch Schweizer Datenschutzrecht. So verlangt auch Art. 6 Abs. 2 revDSG, dass der Auftragsbearbeiter „gleichwertige" Bestimmungen einhalten muss.
Der Exporteur kann nicht „sicherstellen", dass der Empfänger die Standarddatenschutzklauseln beachtet; er kann nur, aber immerhin, darauf hinwirken.
Dies ist in den Erläuterungen (S. 28) unter Hinweis auf das BJ entsprechend festgehalten und sollte zur Klarstellung auch in die Verordnung einfliessen.

Der risikobasierte Ansatz bei der Beurteilung von Datentransfers in Länder ohne angemessenen Datenschutz auf Grundlage der SCC ist zu bejahen. Allerdings ist dieser Ansatz mit Blick auf die Praxishinweise der EU-Behörden keinesfalls selbstverständlich. Entsprechend bedarf es einer Klarstellung in der Verordnung zur Schaffung von Rechtssicherheit.

Formulierungsvorschlag:
Klarstellung im Erläuterungsbericht, dass der Empfänger nicht verpflichtet werden muss, „die schweizerischen Datenschutzvorschriften" einzuhalten.
Und
1 Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Abs. 2 Buchstabe d DSG ins Ausland bekannt, so ~~trifft er angemessene Massnahmen, um sicherzustellen~~ trägt er in angemessener Weise Sorge für deren Einhaltung.

2. Kapitel: Pflichten der Verantwortlichen ~~und des Auftragsbearbeiters~~
Da die Pflichten des Auftragsbearbeiters aus Sicht der Wirtschaft zwingend gestrichen werden sollten, muss auch der Titel von Kapitel 2 angepasst werden.

Artikel 13 (Modalitäten der Informationspflicht)

Antrag economiesuisse:
1) Streichung des Auftragsbearbeiters

Und
2) Ergänzung der Möglichkeit eine Information auch elektronisch zur Verfügung zu stellen.

Und

3) Streichung der unpräzisen Vorgaben für eine angemessene Information und Streichung der unklaren Anforderungen an Piktogramme.

Begründung:

1) Die Informationspflicht gegenüber den betroffenen Personen kann nur den Verantwortlichen treffen. Die vorgeschlagene Regelung steht im diametralen Widerspruch zum neuen DSG (Art. 19 revDSG) (!) und der DSGVO (Art. 13 und 14). In beiden Gesetzen trifft die Informationspflicht – selbstverständlich - nur den Verantwortlichen. Der Auftragsbearbeiter muss und kann nicht informieren, und er darf es auch gar nicht, ausser auf Weisung und in Vertretung des Verantwortlichen. Im Übrigen ist diese Pflicht strafbewehrt (Art. 60 revDSG), so dass auf diesem Weg auch die Strafbarkeit des Auftragsverarbeiters bzw. der für ihn handelnden Personeneingeführt würde. Dafür bräuchte es aus rechtstaatlichen Gründen zwingend ein Gesetz im formellen Sinn, was die VDSG nicht ist.
   Es ist zudem unzutreffend, dass die Pflichtangaben «mitzuteilen» sind. Es geht bei der Datenschutzinformation nicht um eine Mitteilung wie bei bestimmten rechtgeschäftlichen Erklärungen, die dem Empfänger zugehen müssen (vgl. z.B. Art, 40e Abs. 4, Art. 176 Abs. 2 oder Art. 269d OR), sondern darum, eine bestimmte Situation – die Bearbeitung – nach aussen erkennbar zu machen. Vergleichbar ist dies mit der Deklaration von Konsumenteninformationen (vgl. Art. 1 lit. a KIG). Bei Art. 13 Abs. 1 E-VDSG ist deshalb von «zur Verfügung stellen» zu sprechen anstelle von «mitteilen».
2) Das revDSG sieht nicht vor, dass die Betroffenen die „wichtigsten Informationen“ auf der „ersten Kommunikationsstufe“ erhalten müssen (vgl. aber Erläuterungen, S. 30). Vielmehr hält revDSG Art. 19 Abs. 1 fest, die Information müsse „angemessen“ erfolgen. Daraus folgt, dass die Mitteilung von den jeweiligen Umständen abhängig ist. Dabei sind auch Informationsinteresse und die Erwartungen des Betroffenen zu berücksichtigen: Während er damit rechnen mag, dass sich in einem Vertrag ein Hinweis auf die Datenschutzerklärung findet, ist ein solcher auf Visitenkarten, E-Mails oder Briefpapier nicht üblich. Sollte sich eine Person ausnahmsweise dafür interessieren, kann ihr ohne weiteres zugemutet werden, z.B. die Webseite des betreffenden Unternehmens zu konsultieren. Darum darf es nicht erforderlich sein, in Alltagssituationen – wie bei einer Terminvereinbarung, am Schalter – explizit auf die Datenschutzerklärung hinweisen zu müssen. Dabei ist der Standard «auf Papier oder elektronisch zur Verfügung stellen» zu wählen, welcher in neueren Gesetzen wie z.B. FIDLEG bereits genutzt wurde. Zudem wäre ohnehin unklar, welches die «wichtigsten Informationen» sind.
3) Weil Piktogramme ohnehin nur ergänzend verwendet werden dürfen, sind daran keine zusätzlichen Anforderungen zu stellen. Zumal aufgrund der Erläuterungen nicht klar ist, was mit „maschinenlesbar“ gemeint ist.

Formulierungsvorschlag

1 Der Verantwortliche ~~und der Auftragsbearbeiter teilen~~ stellt die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form auf Papier oder elektronisch zur Verfügung.

~~2 Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~

Artikel 15 (Information bei der Bekanntgabe von Personendaten)

Antrag economiesuisse:
Ersatzlos streichen

Begründung:
Art. 15 E-VDSG statuiert völlig neue formale zusätzliche Modalitäten und Zusatzpflichten in Zusammenhang mit der Bekanntgabe von Daten an Dritte, welche strikt regelbasiert ohne Differenzierungsmöglichkeit in jedem Fall anwendbar sein sollen. Hierzu findet sich im revDSG keine gesetzliche Grundlage. Im Gegenteil hat das Parlament die Bekanntgabe von Personendaten an Dritte bereits auf Gesetzesstufe an verschiedenen Stellen ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt (vgl. namentlich Art. 16 ff. revDSG). Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen.

Die Regelung würde inhaltlich zu massiven Zusatzanforderungen bei jeder Art von Kommunikation im Zusammenhang mit Personendaten, z.B. bei jedem einzelnen E-Mail, führen. Damit würde an übliche und vernünftige Kommunikation, selbst solche ohne erkennbare datenschutzrechtliche Risiken, völlig überrissene Anforderungen gestellt. Im operativen Alltag würden damit etablierte, übliche und vernünftige Kommunikationsmittel wie z.B. E-Mail de facto gänzlich verhindert. Solche Anforderungen stehen in vollständigem Widerspruch zu den Anstrengungen des Bundesrats, Digitalisierung und Innovationskraft im Interesse des Wirtschaftsstandorts Schweiz zu fördern.
Dementsprechend finden sich auch im EU-Recht, auf welches sich der Erläuterungsbericht zu Unrecht beruft, keine solchen Pflichten für private Datenbearbeiter. Art. 15 E-VDSG ist mithin ein für das wesentliche Regulierungsziel EU-Äquivalenz kontraproduktiver "Swiss Finish".

Somit ist die Regelung am besten gänzlich zu streichen, zumindest aber ausdrücklich auf Bundesorgane einzugrenzen.

Sofern die Regelung nicht gänzlich gestrichen wird, ist zudem auch hier der Auftragsbearbeiter – wie bereits erwähnt – jedenfalls nicht Adressat der Informationspflicht und ist deshalb zu streichen. Der Auftragsbearbeiter verfügt weder über die entsprechenden Angaben noch ist er zu einer solchen Mitteilung befugt, es sei denn auf Weisung und in Vertretung des Verantwortlichen.

Artikel 16 (Information über die Berichtigung, Löschung und Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten)

Antrag economiesuisse:
Ersatzlos streichen

Begründung:
Die Pflicht wurde im Rahmen der Vernehmlassung zum revDSG gestrichen und darf nun nicht über die VDSG wieder eingeführt werden. Zudem besteht keine Notwendigkeit, da der Verantwortliche bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten hat, ebenso wie die Empfänger von Personendaten.

Darum ist Art. 16 E-VDSG zu streichen.

Artikel 17 (Überprüfung einer automatisierten Einzelentscheidung)

Antrag economiesuisse:
Ersatzlos streichen

Begründung:
Dieser Artikel stellt unseres Erachtens einen Eingriff in die Privatrechtsautonomie dar und darf daher nicht auf Verordnungsstufe verankert werden.

Zudem geht die Regelung von falschen rechtlichen Voraussetzungen aus. Ein generelles Diskriminierungsverbot gibt es nicht. Soweit es direkt aus Grundrechten der Verfassung abgeleitet werden sollte, wäre dies unzulässig, da es keine direkte Drittwirkung verfassungsmässiger Rechte auf Private gibt. Eine Diskriminierung wird rechtlich erst dann kritisch, wenn sie rein subjektiv ohne sachlich überzeugende Abgrenzungskriterien erfolgt. All dies ist aber schon deshalb nicht auf Stufe E-VDSG zu regeln, weil das Thema allgemeiner Natur ist und in sämtlichen Rechtsmaterien gleichermassen eine Rolle spielt. Nur schon die etablierte bundesgerichtliche Praxis zum Thema gibt ausreichende Rechtssicherheit.
Eine weitere Präzisierung von Art. 21 revDSG auf Stufe E-VDSG ist weder sinnvoll noch nötig und mangels gesetzlicher Grundlage auch nicht zulässig. Das Parlament hat die Anforderungen an die Informationspflichten bei automatisierten Einzelentscheiden in Art. 21 revDSG bereits ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt. Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen.
Nach alledem gleichwohl eine solche Regel in die E-VDSG einzuführen, würde unnötigerweise erhebliches Potential für missbräuchliche Klagen gegen Verantwortliche produzieren, welche sich effektiv absolut korrekt und gesetzeskonform verhalten hatten.

Art. 17 E-VDSG ist demnach ersatzlos zu streichen.

Artikel 18 (Form und Aufbewahrung der Datenschutz – Folgeabschätzung)

Antrag economiesuisse:
Die Aufbewahrungsfrist ist zu streichen und «schriftlich» zu präzisieren.

Begründung:
Wie in anderen modernen Gesetzen auch sollte der Begriff der Schriftlichkeit dahingehend präzisiert werden, dass auch andere Formen erfasst werden, die den Nachweis durch Text ermöglichen.

Die Aufbewahrungspflicht sollte im zweiten Satz von Art. 18 E-VDSG mangels gesetzlicher Grundlage im revDSG gestrichen werden. Ausserdem besteht unseres Erachtens aufgrund des Grundsatzes der Verhältnismässigkeit der Datenbearbeitung sowie der Datenminimierung kein Grund, eine Datenschutz-Folgenabschätzung während zwei Jahren nach Beendigung der Datenbearbeitung aufzubewahren. Schliesslich widersprechen die Ausführungen im Erläuterungsbericht dem nemo-tenetur-Grundsatz, sollten die Datenschutz-Folgenabschätzung zu Beweiszwecken gegen den Verantwortlichen aufbewahrt werden. Sollte an den zwei Jahren festgehalten werden, müsste mindestens die Ergänzung «während mindestens zwei Jahren» oder «für einen angemessenen Zeitraum» eingesetzt werden, sodass eine allfällige längere Aufbewahrung der Daten nicht als datenschutzwidrig gilt.

Formulierungsvorschlag:
1 Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in anderer durch Text nachweisbarer Form festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~

Artikel 19 (Meldung von Verletzungen der Datensicherheit)

Antrag economiesuisse:

1) Lit. e und lit. f sind zu präzisieren.
2) Streichung der über das Gesetz hinausgehenden generellen Pflicht, die betroffene Person zu informieren.
3) Streichung der gesetzlich nicht vorgesehenen Dokumentationspflicht nach VDSG Art. 19 Abs. 5.
4) Anpassung Erläuterungsbericht: Die Auslegung des Begriffs „voraussichtlich" ist falsch und zu korrigieren.

Begründung:

1) Lit. e ist falsch formuliert. Die «allfälligen Risiken» beinhalten bereits die Folgen für die betroffenen Personen. Richtig müsste es heissen: «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht». Auch in lit. f muss nicht von den «Folgen», sondern vom «Risiko» die Rede sein. Gemildert werden kann entweder das Schadensausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem «Risiko» entspricht). Bei lit. f ist zudem zu präzisieren, dass es nur um Massnahmen gehen kann, welche der Verantwortliche tatsächlich ergriffen hat ("gegebenenfalls").
2) Art. 19 Abs. 2 E-VDSG geht über Art. 24 Abs. 4 revDSG hinaus. Während das Gesetz eine Information der betroffenen Person nur vorschreibt, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt, sieht die Verordnung vor, dass der Verantwortliche den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mitteilt. Zusätzlich besteht keine gesetzliche Grundlage (Mindestangaben, Dokumentationspflicht) und es entsteht ein Swiss Finish (Angabe von Zeitpunkt und Dauer der Verletzung).
3) Die Dokumentationspflicht gemäss Art. 19 Abs. 5 E-VDSG entbehrt einer gesetzlichen Grundlage und sollte folglich ersatzlos gestrichen werden. Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen Swiss Finish darstellt. Falls an der Dokumentationspflicht festgehalten werden sollte, ist zu präzisieren, dass nur meldepflichtige Verletzungen aufzubewahren sind.
4) „Voraussichtlich" heisst nicht, dass „in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, eine Meldung erfolgen muss" (so die Erläuterungen, S. 32). Der Begriff „voraussichtlich" setzt vielmehr voraus, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko führt. Der Erläuterungsbericht sollte so berichtigt werden, dass in Fällen, wo das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, nicht gemeldet werden muss, sondern nur dann, wenn die Verletzung der Datensicherheit höchstwahrscheinlich zu einem hohen Risiko führt.

Formulierungsvorschlag:
1 Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit:
a. die Art der Verletzung;
b. soweit möglich den Zeitpunkt und die Dauer;
c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;
d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;

e. die Folgen, ~~einschliesslich der allfälligen Risiken~~, für die betroffenen Personen, von welchen ein hohes Risiko ausgeht;
f. gegebenenfalls welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder ~~die Folgen~~ das Risiko zu mildern;
g. den Namen und die Kontaktdaten einer Ansprechperson.
2 Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.
3 ~~Der~~ Falls der Verantwortliche verpflichtet ist, die ~~teilt den~~ betroffenen Personen zu informieren, so teilt er ihnen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit.
4 […]
~~5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.~~

3. Kapitel: Rechte der betroffenen Person

Artikel 20 (Modalitäten)

Antrag economiesuisse:

1) Die Auskunftserteilung sollte nicht nur schriftlich, sondern auch in einer anderen durch Text nachweisbaren Form möglich sein.
2) Aufnahme der Präzisierung, dass der Begriff „Daten als solche“ insbesondere auch eine Auskunft in aggregierter Form zulässt.
3) Ergänzung bzw. Umformulierung von Abs. 3.
4) Dokumentationspflicht nach Art. 20 Abs. 5 ist zu streichen.

Begründung:

1) In den Erläuterungen (S. 34) wird festgehalten: „Es kann hier ferner präzisiert werden, dass zur schriftlichen Form auch die elektronische Form gehört.“ Diese Präzisierung ist in die Verordnung aufzunehmen.
2) In den Erläuterungen (S. 35) wird ausgeführt: „Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Die mündliche Mitteilung von Informationen, zum Beispiel am Telefon, ist ebenfalls möglich, sofern die betroffene Person eingewilligt hat.“ Es besteht im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten bzw. Unterlagen. Vielmehr ist die Mitteilung nach entsprechender Debatte vom Gesetzgeber bewusst beschränkt worden auf die „bearbeiteten Personendaten als solche“ (Art. 25 Abs. 2 lit. b revDSG). Damit soll namentlich auch die Auskunft in aggregierter Form ermöglicht werden. Dies sollte zwecks Präzisierung in der Verordnung verankert werden.
3) Betreffend Art. 20 Abs. 3 E-VDSG haben die Mitglieder von economiesuisse zwei verschiedene Vorgehensweisen, um eine Anpassung im Sinne der Wirtschaft vorzunehmen. Einige Mitglieder sprechen sich für eine Streichung des Absatzes aus, während Andere eine Streichung unterstützen würden, aber alternativ für eine Umformulierung plädieren.

Option 1: Streichung
Für eine komplette Streichung spricht, dass das Gesetz bereits eine Auskunft an die betroffene Person vorschreibt und auch den Umfang und die Art dieser Auskunft bereits klar und deutlich definiert. Die

betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Eine weitere Pflicht des Verantwortlichen, einer betroffenen Person diese Auskunft auch noch „verständlich“ zu machen, entbehrt einer gesetzlichen Grundlage. Nachdem das Gesetz den Mindestumfang der Auskunft im Detail beschreibt, ist diese zusätzliche Anforderung in der Verordnung auch gar nicht notwendig, dürfte eine Auskunft, welche den gesetzlichen Vorgaben entspricht, regelmässig für jeden Durchschnittsadressaten verständlich sein. Diese Verordnungsbestimmung schiesst zudem über das Ziel hinaus, vgl. Begründung in der Wegleitung: «Werden Personendaten in einer technischen Form geliefert, die für die betroffene Person nicht lesbar und/oder nicht verständlich ist, muss der Verantwortliche imstande sein, ihr ergänzende Erläuterungen zu geben, beispielsweise mündlich.»

Option 2: Umformulierung
Art. 20 Abs. 3 E-VDSG verlangt, dass die Auskunft verständlich sein muss. Dies bedeutet nicht, dass der Verantwortliche der um Auskunft ersuchenden Person die Datensätze oder darüber hinaus gehend sogar die damit einhergehenden Abläufe und Geschäftsmodelle erklären muss. Dies könnte im Einzelfall je nach Person mit enormem und unverhältnismässigem Aufwand verbunden sein und wäre je nach Person u.U. gleichwohl untauglich. Zudem könnte eine solche Regelung auch dazu missbraucht werden, das Verfahren und damit den Aufwand für den Verantwortlichen ohne sachlichen Grund "künstlich" zu verlängern.
Vielmehr muss ausreichend sein, die herauszugebenden Daten so aufzubereiten und darzustellen, dass sie geordnet sind und dadurch unter Anwendung eines objektivierten Masstabes nach Treu und Glauben verständlich sind oder sein müssen. Ob die betroffene Person diese Darstellung im konkreten Fall tatsächlich versteht, kann nicht relevant sein, geht es doch beim datenschutzrechtlichen Auskunftsbegehren nur darum, die bearbeiteten Daten mitzuteilen. Dies entspricht dem Kern des Auskunftsanspruchs, welcher die effektive Herausgabe der relevanten Daten sicherstellt. Darüber hinaus besteht keine Pflicht des Verantwortlichen, die Daten, deren Zweck oder – damit zusammenhängend – die Art der Datenhaltung oder sogar die Geschäftsabläufe zu erläutern. Solches ist schon deshalb abzulehnen, weil dadurch der Aufwand unermesslich und im Einzelfall sogar "never ending" werden könnte. Beispielsweise können die im Rahmen einer klinischen Studie bearbeiteten Daten oder technische Logdaten für die betroffene Person unverständlich sein. Müssen diese zuerst so dargestellt werden, dass sie für die betroffene Person verständlich sind, kann dies oft nicht innerhalb von 30 Tagen erfolgen. Damit würde der Grundsatz der Auskunftserteilung innert 30 Tagen entgegen der gesetzlichen Absicht regelmässig zur Ausnahme.
Will die auskunftsberechtigte Person mehr über solche über den eigentlichen Herausgabeanspruch hinaus gehende Verhältnisse erfahren, muss sie sich an einen Rechtsanwalt oder Wirtschaftsfachmann halten, nicht an den Verantwortlichen. Demzufolge ist Abs. 3 zusätzlich dahingehend zu klären, dass über die eigentliche "geordnete" Datenherausgabe "keine zusätzlichen Erläuterungen erforderlich" sind.
Da die Aktivität und die damit einhergehende Verständlichkeit der Auskunft vom Verantwortlichen ausgeht und von diesem gesteuert werden kann und muss, macht es Sinn, den Verantwortlichen hier bei Abs. 3 mit Bezug auf die Formulierung in den Aktiv-Modus zu setzen.

Die Dokumentationspflicht nach Art. 20 Abs. 5 E-VDSG entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen Swiss Finish darstellt. Die Regelung ist ferner unnötig, da aufgrund der Beweislast ohnehin im Interesse des Verantwortlichen, mit Dokumentation den Nachweis erbringen zu können.

Formulierungsvorschlag:
3 ~~Die Auskunft muss für die betroffene Person verständlich sein.~~ Der Verantwortliche muss die Auskunft geordnet vornehmen. Zusätzliche Erläuterungen sind nicht erforderlich.
Oder
~~3 Die Auskunft muss für die betroffene Person verständlich sein.~~

4 Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.

~~5 Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.~~

Artikel 21 (Zuständigkeit)

Antrag economiesuisse:
1) Streichung Abs. 1 Satz 2
2) Konkretisierung Abs. 2

Begründung:
1) Der erste Satz von Art. 21 Abs. 1 E-VDSG ist inhaltlich richtig und nicht zu beanstanden. Der zweite Satz stellt demgegenüber eine Forderung auf, welche im operativen Alltag regelmässig gar nicht erfüllt werden kann. In manchen Konstellationen ist für einen Verantwortlichen weder klar noch eindeutig ersichtlich, inwieweit für einen bestimmten Sachverhalt ein anderer Verantwortlicher zuständig sein soll und wer dies gegebenenfalls ist. In vielen Fällen kann ein Verantwortlicher deshalb der Pflicht, das Begehren an den zuständigen Verantwortlichen weiterzuleiten, naturgemäss gar nicht nachkommen. In unklaren Fällen ein Auskunftsbegehren an andere, vermeintlich zuständige Verantwortliche weiterzuleiten, würde dem Datenschutz geradezu entgegenlaufen, erhielten doch auf diese Weise womöglich Personen Kenntnis vom Fall, welche gar nicht als Verantwortliche qualifizieren. Einer fälschlicherweise um Auskunft ersuchten Person ist es auch nicht zuzumuten, abzuklären, wer an seiner Stelle Verantwortlicher sein könnte. Auch solche Abklärungen würden dem berechtigten Bedürfnis der um Auskunft ersuchenden Person nach Einhaltung des Datenschutzes gerade zuwiderlaufen.

2) Auftragsbearbeiter sind nicht darauf eingerichtet, Auskunft zu erteilen, weil sie keine entsprechende gesetzliche oder vertragliche Pflicht haben. Der Verweis auf eine Auskunftserteilung durch den Auftragsbearbeiter ist deshalb falsch und kann in der Praxis deshalb Probleme schaffen. Gemeint ist hier wohl vielmehr, dass Auftragsbearbeiter den Verantwortlichen bei der Auskunftserteilung unterstützen sollen, was in der Praxis ohnehin jeweils so vereinbart wird. Des Weiteren ist Art. 21 Abs. 2 E-VDSG verwirrlich, da er impliziert, dass der Auftragsbearbeiter selbst eine Auskunftspflicht hat, wenn er faktisch in der Lage sein sollte, eine Auskunft zu erteilen bzw. er das Auskunftsgesuch in einem solchen Fall nicht weiterleiten muss, auch wenn er es nicht beantwortet. Das kann nicht sein. Im Gegenteil ist es dem Auftragsbearbeiter i.d.R. vertraglich untersagt, selbst Auskunft zu erteilen, wenn ein Auskunftsbegehren direkt bei ihnen eingehen sollte. Der letzte Halbsatz von Abs. 2 ("sofern er nicht in der Lage ist, selbst Auskunft zu geben") ist zu streichen und durch die Formulierung "sofern er das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet" zu ersetzen.

Formulierungsvorschlag:

1 Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. ~~Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.~~

2 Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so unterstützt der Auftragsbearbeiter den Verantwrotlichen~~leitet der Verantwortliche das Begehren zur~~ bei der Erteilung der Auskunft ~~Erledigung an den Auftragsbearbeiter weiter,~~ sofern er ~~nicht in der Lage ist, selbst Auskunft zu erteilen~~das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet.

Artikel 22 (Frist)

Antrag economiesuisse:
Der Fristbeginn ist zu präzisieren.

Begründung:
Wenn aus dem Auskunftsbegehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, soll die Frist erst mit dieser Klarstellung zu laufen beginnen. Zudem ist klarzustellen, dass erst der Eingang des Begehrens beim Verantwortlichen fristauslösend ist und nicht etwa beim Auftragsbearbeiter, falls ein Betroffener das Begehren dem Auftragsbearbeiter zugestellt und dieser das Begehren dem Verantwortlichen weiterleitet.

Formulierungsvorschlag:
1 Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens beim Verantwortlichen erteilt. Erfordert das Begehren einer Präzisierung, welche Daten die betroffene Person wünscht, beginnt die Frist mit Zugang der Präzisierung beim Verantwortlichen zu laufen. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen.

Artikel 23 (Ausnahme von der Kostenlosigkeit)

Antrag economiesuisse:

1) Der Maximalbetrag von CHF 300.- ist zu streichen.
2) Der Fristbeginn sollte ergänzt werden, um die 30 Tage sicherzustellen.

Begründung:

1) Der Maximalbetrag von CHF 300.-- wird den tatsächlichen Verhältnissen und dem damit verbundenen Aufwand nicht ansatzweise gerecht. Sind z.B. zur Sicherstellung des Datenschutzes von Dritten umfangreiche Schwärzungen notwendig, kann dies im Einzelfall durchaus höhere Aufwendungen mit sich bringen. Art. 23 Abs. 2 E-VDSG sollte deshalb gestrichen werden, da die die angemessene Kostenbeteiligung bereits in Abs. 1 enthalten ist und keine weiteren Einschränkungen nötig sind.
2) Abs. 3 muss dahingehend angepasst werden, dass die in Abs. 1 geregelte Frist von 30 Tagen zur Auskunftserteilung nicht faktisch auf 20 Tage abgekürzt werden kann. Dies kann durch eine Ergänzung des Fristbeginns in Abs. 3 sichergestellt werden.

Formulierungsvorschlag:
1 Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden, oder querulatorisch ist.
~~2 Die Beteiligung beträgt maximal 300Franken.~~
3 Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen. Die Frist zur Auskunftserteilung beginnt mit Ablauf der Rückzugsfrist.

4. Kapitel: Rechte der betroffenen Person

Artikel 25 (Datenschutzberaterin und Datenschutzberater)

Antrag economiesuisse:

1) Art. 25 Abs. 1 lit. b E-VDSG ist ersatzlos zu streichen. Dementsprechend kann Art. 25 Abs. 1 lit. a E-VDSG direkt in Abs. 1 integriert werden.
2) Das Interventionsrecht gemäss lit. b ist zur Vervollständigung einer konzeptionell in sich stimmigen «Good Governance» mit dem Eskalationsrecht in einer neuen lit. c zu ergänzen.

Begründung:

1) Die gesetzliche Regelung zur Funktion der Datenschutzberatung wird auf Verordnungsstufe eingeengt.
   Die Datenschutzberaterin oder der Datenschutzberater muss lediglich beratend Einfluss nehmen, damit der Verantwortliche die Datenschutzpflichten richtig anwendet (vgl. Art. 10 revDSG, insb. Abs. 2 lit. b). Bei der Formulierung von Art. 25 Abs. 1 lit. a E-VDSG bleibt mit der Formulierung "prüft" der Umfang der Prüfpflicht unklar. Die Funktion Datenschutzberatung kann jedenfalls nicht jede beim Verantwortlichen anfallende Datenbearbeitung prüfen. Der Verantwortliche kann aber in Absprache mit der Funktion Datenschutzberatung eine interne Governance schaffen, welche in geeigneter Form die internen Regeln zu diesem Thema festlegt. So sollte die Funktion Datenschutzberatung nur solche Datenbearbeitungen prüfen, welche ihr effektiv vorgelegt werden. Dies auch zum eigenen Schutz. Ausserhalb der Konsultationspflicht muss die Funktion Datenschutzberatung entsprechend ihrer Hauptfunktion nur allgemein beratend tätig sein. Zur Klarstellung dieser Verhältnisse ist - auch zum Schutz von Datenschutzberatern, für welche keine spezifische interne Governance besteht - die in Art. 25 Abs. 1 lit. a genannte Prüfpflicht auf "ihm vorgelegte" Datenbearbeitungen einzugrenzen.

   Die Regelung von Art. 25 Abs. 1 lit. b E-VDSG widerspricht der Funktion Datenschutzberatung und überdies der Organisationsfreiheit des Verantwortlichen, wie genau die Pflichten gemäss revDSG unter Würdigung der konkreten Verhältnisse im Unternehmen personell, technisch und organisatorisch am besten erfüllt werden sollen. Insofern liegt ein nicht stufengerechter Eingriff in die Privatautonomie des Unternehmens als Verantwortlichem vor.
   Ferner verletzt die Bestimmung das weltweit als Standard etablierte drei Linien Verteidigungsmodell, in dem es die Erkennung, Einhaltung und Korrektur von datenschutzrechtlichen Vorgaben einer einzelnen Funktion, namentlich der Datenschutzberaterin oder dem Datenschutzberater, auferlegt.

   Schliesslich macht die vorgeschlagene Regelung von Art. 25 Abs. 1 lit. b E-VDSG die übergeordnete Ausnahmeregelung von Art. 23 Abs. 4 revDSG obsolet oder anders gesagt: Art. 25 Abs. 1 lit. b E-VDSG ist gar nicht nötig, weil mit Art. 23 Abs. 4 revDSG bereits eine ausreichende übergeordnete Regelung besteht.

Nach alledem ist Art. 25 Abs. 1 lit. b E-VDSG ersatzlos zu streichen. Dementsprechend kann Art. 25 Abs. 1 lit. a E-VDSG direkt in Abs. 1 integriert werden, was die Regelung etwas kürzer macht.

2) Art. 25 Abs. 2 lit. b E-VDSG regelt zu Recht ein Interventionsrecht. Dies ist nötig, damit die Datenschutzberaterin oder der Datenschutzberater bei unternehmensinternen Prüfungen der Einhaltung datenschutzrechtlicher Regeln nicht nur den Worten bzw. den ihr oder ihm zur Verfügung gestellten Dokumenten vertrauen muss, sondern – soweit sinnvoll und nötig – die Beschaffung zusätzlicher Informationen und Dokumente durchsetzen kann. Mit dieser Regelung bleibt Art. 25 Abs. 2 lit. b E-VDSG aber «auf halbem Weg» stehen. Stösst die Datenschutzberaterin oder der Datenschutzberater nämlich bei der Ausübung des Interventionsrechts auf Unstimmigkeiten und sind die Linienverantwortlichen nicht gewillt, entsprechend dem Ratschlag der Datenschutzberaterin oder des Datenschutzberaters Abhilfe zu schaffen, muss Letzterer oder Letzterem spiegelbildlich zum Interventionsrecht bzw. zur Vervollständigung des Gesamtprozesses überdies ein Eskalationsrecht zustehen. Ein solches Recht ist sachlogisch keine Pflicht. Die Datenschutzberaterin oder der Datenschutzberater erhält damit aber das notwendige Instrumentarium, zumindest im Fall komplexer Verhältnisse und besonders schwerwiegende Verstösse gegen Datenschutzpflichten notfalls, mithin als Ausnahme von der Regel, die Thematik im Rahmen und allenfalls in Absprache mit der Compliance-Organisation, soweit eine solche besteht, auf dem Linienweg nach oben zu eskalieren und auf diese Weise auf höherer Stufe zum Entscheid zu bringen bzw. bringen zu lassen, nötigenfalls bis zum höchsten Organ des Unternehmens, und damit klare Verhältnisse zu schaffen. Bei einfacheren Strukturen genügt es aber auch, wenn die Funktion Datenschutzberatung in wichtigen Fällen die höchsten Organe lediglich informiert. Andernfalls setzt sich die Datenschutzberaterin oder der Datenschutzberater gerade bei schwerwiegenden Verstössen gegen Datenschutzpflichten dem Risiko aus, mangels Eskalationsmöglichkeit im Schadensfall selbst haftbar zu werden, weil ihr oder ihm vorgeworfen wird, sich nicht hartnäckig genug eingesetzt zu haben.
Art. 25 Abs. 2 E-VDSG ist somit mit einer lit. c zu ergänzen, welche ergänzend zum Interventionsrecht nach lit. b das Eskalationsrecht regelt.

Formulierungsvorschlag:
1 Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen ~~muss folgende Aufgaben wahrnehmen:~~
~~a.~~ ~~Sie oder er~~ prüft die ihm vorgelegten Bearbeitungen von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass rechtliche Datenschutzvorschriften verletzt wurden.
~~b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.~~
2 Der private Verantwortliche muss der Datenschutzberaterin oder dem Datenschutzberater:
a. die notwendigen Ressourcen zur Verfügung stellen;
b. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.
c. das Recht einräumen, in wichtigen Fällen die höchsten Organe zu informieren.

Artikel 26 (Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten)

Antrag economiesuisse:
Es ist zu präzisieren, dass sich die allfällige Pflicht eines KMU zur Führung eines Verzeichnisses nicht auf sämtliche Bearbeitungen erstreckt, sondern auf diejenigen Bearbeitungen beschränkt ist, welche die Voraussetzung(en) triggern.

Begründung:
Der Bundesrat hat gemäss Art. 12 Abs. 5 revDSG Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses vorzusehen für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und deren Datenbearbeitung ein „geringes Risiko" mit sich bringt. Gemäss E-VDSG 26 bedeutet ein geringes Risiko, dass weder „umfangreich besonders schützenswerte Personendaten bearbeitet" werden noch „ein Profiling mit hohem Risiko durchgeführt" wird. Alle anderen Bearbeitungen bringen im Umkehrschluss ein geringes Risiko mit sich. Durch Präzisierung, dass sich die Pflicht zur Führung eines Verzeichnisses ausschliesslich auf diejenigen Bearbeitungen erstreckt, welche die Voraussetzung triggern, kann sowohl dem Schutz der betroffenen Personen als auch den Bedürfnissen der KMU angemessen Rechnung getragen werden (vgl. auch das Positionspapier des EDSA zu Art. 30 Abs. 5 DSGVO).

Es ist ferner zu präzisieren, dass das Verzeichnis nicht schriftlich, sondern auch in anderer Form, die den Nachweis durch Text ermöglicht, z.B. elektronisch, geführt werden kann. Damit ist klargestellt, dass das Verzeichnis auch elektronisch geführt werden kann.

Formulierungsvorschlag:
1 Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:
a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet.
b. Es wird ein Profiling mit hohem Risiko durchgeführt.
2 Ist eine Voraussetzung nach Abs. 1 lit. a und/oder b erfüllt, so ist die Verzeichnispflicht auf diejenige bzw. diejenigen Bearbeitung bzw. Bearbeitungen beschränkt, welche dieser bzw. diesen Voraussetzung bzw. Voraussetzungen zugrunde liegen.
3Das Bearbeitungsverzeichnis ist schriftlich, oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu führen.

7. Kapitel: Schlussbestimmungen

Antrag economiesuisse:
Das lückenhafte Übergangsregime auf Stufe des revDSG ist auf Verordnungsstufe mit zusätzlichen Übergangsbestimmungen zu ergänzen.

Begründung:
Für sämtliche neuen Pflichten, welche erheblichen Aufwand generieren, müssen angemessene Übergangfristen bestehen, zumal IT-gestützte Lösungen nötig sind.
Dabei ist zu berücksichtigen, dass die verschiedenen Regeln und Pflichten des gesamten Regelwerks (Gesetz samt Verordnung) gegenseitige Wechselwirkungen generieren. Die neuen Regeln bzw. Pflichten sind deshalb zusammen mit den unverändert weiter geltenden Regeln bzw. Pflichten zu einem in sich stimmigen Gesamtkonzept zu verschmelzen. Ein solches Gesamtkonzept kann sachlogisch erst

nach Vorliegen der finalen Texte auf Gesetzes- und Verordnungsstufe erarbeitet, final festgelegt und umfassend in die IT-Sprache «übersetzt» werden. Erst danach kann mit dem Aufbau der IT-gestützten Lösung begonnen werden. Vor der «Go live»-Schaltung sind sodann die nach bewährten Standards vorgesehenen Tests durchzuführen. Parallel dazu sind auch die Mitarbeitenden entsprechend ihrer jeweiligen Funktion auszubilden und überdies die Verträge mit Lieferanten und Geschäftspartnern anzupassen.
Für alle diese notwendigen Aktivitäten ist gemäss etablierten Erfahrungswerten ein Zeitraum von rund 2 Jahren ab Vorliegen der finalen Gesetzes- und Verordnungstexte notwendig. Im Gegenzug stellt eine solche IT-gestützte Lösung die gleichförmige Anwendung sämtlicher Regeln innerhalb des gesamten Unternehmens sicher.
Aus den genannten Gründen hat die EU seinerzeit entschieden, für die Umsetzung der EU-DSGVO nicht Übergangsfristen für einzelne Regeln bzw. Pflichten, sondern pauschal 2 Jahre für das gesamte Regelwerk zuzugestehen.

In der Schweiz hat das Parlament für das revDSG eine andere Grundentscheidung getroffen (vgl. Art. 68-74 revDSG). Im Rahmen des parlamentarischen Prozesses liegt der Fokus naturgemäss auf den materiellen Regeln bzw. Pflichten. Das kam beim revDSG besonders deutlich zum Ausdruck, wurde doch über den konkreten Wortlaut einiger zentraler Bestimmungen wie z.B. zum Profiling (Art. 5 lit. f und g revDSG) buchstäblich bis zum Schluss heftig debattiert. Die Übergangsbestimmungen kommen deshalb im parlamentarischen Prozess regelmässig zu kurz, was beim revDSG in erhöhtem Mass der Fall war. Übergangsbestimmungen sollen zudem strikte nach sachlichen Kriterien festgelegt werden und nicht «Spielball» politischer Kompromisse sein. Deshalb hat es sich im schweizerischen Gesetzgebungsprozess inzwischen eingebürgert, falls notwendig ergänzende Übergansbestimmungen oder -fristen auf Verordnungsstufe festzulegen.
Im Zuge der DSG-Revision ist zumindest für folgende entweder neu eingeführten oder zumindest mit neuen Anforderungen konfrontierten Regeln bzw. Pflichten mit offensichtlich erheblichem Umsetzungsbedarf auf Gesetzesstufe keine Übergangsbestimmung festgelegt worden:

- Pflicht, eine angemessene Datensicherheit zu gewährleisten (Art. 8 revDSG i.V.m. Art. 1ff. E-VDSG);
- Pflicht zur Erstellung des Verzeichnisses der Datenbearbeitungstätigkeiten (Art. 12 revDSG);
- Pflicht, so rasch als möglich Meldung von Verletzungen der Datensicherheit zu erstatten (Art. 24 revDSG i.V.m. Art. 19 E-VDSG).

Gerade diese drei zentralen Pflichten können naturgemäss erst gestützt auf das Vorliegen eines umfassenden in sich stimmigen Gesamtkonzepts sämtlicher Regeln bzw. Pflichten zielführend und final festgelegt werden.
Der finale Wortlaut der E-VDSG wird wohl erst gegen Ende des Jahres 2021 vorliegen. Unter Mitberücksichtigung des Umstandes, dass gestützt auf den Wortlaut des revDSG mit den Umsetzungsarbeiten zumindest schon begonnen werden konnte, ist nach dem Gesagten für die beiden vorgenannten Pflichten eine Übergangsfrist bis allermindestens 1. Juli 2023 notwendig, wobei die Aufrechterhaltung der Äquivalenz sichergestellt werden muss.

Formulierungsvorschlag:
Art. 48 ~~Inkrafttreten~~ Übergangsbestimmung betreffend das Verzeichnis der Bearbeitungstätigkeiten und der Meldung von Verletzungen der Datensicherheit
~~Diese Verordnung tritt am ... in Kraft~~. Art. 12 und 24 des Gesetzes sind erst ab 1. Juli 2023 zu erfüllen.

In der Folge würde Art. 48 E-VDSG (Inkrafttreten) neu zu Art. 49 E-VDSG.

Art. ~~48~~49 Inkrafttreten Diese Verordnung tritt am ... in Kraft.

Eventualiter:
Alternativ und zum neuen Art. 48 E-VDSG **zu bevorzugen** kann stattdessen das Inkrafttreten des ganzen Gesetzgebungspakets (revDSG und E-VDSG) nach hinten auf den 1. Juli 2023 geschoben werden (dynamisches Verhältnis zwischen Inkrafttreten und Übergangsfristen).

Da nun schon zwischen dem Abschluss des revDSG und der Vernehmlassung zur VDSG fast ein Jahr verstrichen ist, sollte die Dringlichkeit nicht mehr als Hauptargument einer raschen Inkraftsetzung genannt werden. Zudem brauchen die Unternehmen für die Umsetzung der Verordnung auch ausreichend Zeit. Dies vor allem auf Grund der zusätzlichen Anforderungen, welche durch die VDSG entstehen. Eine Übergangsfrist von mindestens einem Jahr nach Publikation der endgültigen Text von DSG und VDSG erscheint daher als angebracht.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Commission fédérale de la consommation CFC

CH-3003 Berne, CFC

E-Mail
jonas.amstutz@bj.admin.ch

Ihr Zeichen:
Unser Zeichen: voj
Sachbearbeiter/in: teb
Berne, le 11 octobre 2021

Projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) : procédure de consultation

Monsieur Amstutz,

La Commission fédérale de la Consommation (CFC) vous remercie de lui avoir soumis le projet sous rubrique pour prise de position. La CFC a adopté la présente prise de position suite à une analyse détaillée du projet.

D'une manière générale, la CFC souligne **le caractère vague de l'obligation de sécurité** prévu par l'OLPD et son **effet préjudiciable** tant pour les consommateurs que pour les professionnels.

Cette appréciation générale de faiblesse de l'obligation de sécurité est illustrée comme suit :

Le vocabulaire choisi est souvent imprécis ou doit faire l'objet de concrétisations.

- **Art. 2** « dans la mesure du possible »

Il serait bienvenu de circonscrire ce à quoi se rapportent ces termes. *La référence au principe de proportionnalité (p. 17) n'est pas suffisante*.

- **Art. 3** Journalisation

Pour une majorité de la CFC, cet article n'a pas de base évidente dans la nLPD, il présente dès lors une certaine incertitude sur son lien avec la nLPD et dès lors son fondement légal.

Eidgenössische Kommission für Konsumentenfragen
Jean-Marc Vögele
Sekretariat
Bundeshaus Ost, CH-3003 Bern
Tel.: +41 58 462 20 46, Fax: +41 58 462 43 70
jean-marc.voegele@bfk.admin.ch
www.konsum.admin.ch

La CFC propose la **formulation suivante de l'article 3** (proposition en italique):

> « Lorsque l'analyse d'impact sur la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées *et qu'il ne peut être vérifié ultérieurement, par d'autres moyens, que les données ont été traitées aux fins pour lesquelles elles ont été collectées ou divulguées,* le responsable du traitement privé et son sous-traitant journalisent au moins les opérations suivantes: enregistrement, modification, lecture, communication, effacement ou destruction. »

- **Art. 4 al. 1 let. a** "traitement de données sensibles *à grande échelle* »

Le terme « à grande échelle » se retrouve à l'art. 26 let. a OLPD sans que l'on sache quand le traitement de telles données n'a pas lieu de cette façon. *Il faut donc préciser la portée de cette notion.*

- **Art. 4 al. 3** « … sous une forme qui lui est *intelligible* »

Qu'entend-on par cet adjectif ? Le caractère intelligible est-il apprécié de manière objective ou du point de vue de chaque destinataire ? *La formulation doit être précisée.*

- **Art. 6** Modalités

La CFC propose une formulation plus claire :

> al.1 « Le responsable du traitement qui confie un traitement de données personnelles à un sous-traitant demeure responsable de la protection des données. Il ne travaille qu'avec des sous-traitants mandatés qui offrent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement soit effectué conformément aux exigences de la nLPD et assure la protection des droits fondamentaux de la personne concernée. »

- **Art. 9 al. 2** « le responsable du traitement prend les *mesures adéquates* »

La notion est trop imprécise. Des précisions sur ce que le législateur entend par « mesures adéquates » permettrait au responsable du traitement, comme à la personne concernée d'évaluer, si tel est le cas dans une situation particulière. Evidemment, la jurisprudence donnera des indications. Toutefois, *quelques exemples concrets* seraient bienvenus afin d'augmenter la sécurité juridique.

- **Art. 10 al. 1** « (…) le responsable du traitement prend les *mesures adéquates* (…) »

Il serait bienvenu de donner des *indications sur les critères* pour apprécier si les mesures sont adéquates.

- **Art. 13 al. 2**

Que signifie « être lisibles par la machine » ? S'agit-il de la traduction en code binaire ?

- **Art. 16** « implique des efforts disproportionnés »

Comment déterminer si des efforts sont ou non proportionnés ? *Il faudrait indiquer quelques critères.*

- **Art. 20** « (…) doivent être *compréhensibles* pour la personne concernée »

Faut-il se placer du point de vue de cette personne ? Par exemple s'agissant de la langue ou du niveau d'éducation ? ou l'appréciation est-elle objective ?

Enfin, dans le prolongement des remarques mentionnées ci-dessus, **l'articulation entre l'art. 2 et l'art. 3** n'est pas aisée. On pourrait être tenté de conclure que l'obligation de journalisation ne repose sur aucune base légale. Il semble toutefois qu'il s'agit là d'une nouvelle strate apportée à l'obligation de sécurité, si le niveau exigé ne peut être réalisé selon les prescriptions de l'art. 2.

De l'avis de la CFC, la mesure revêt une **importance majeure**, sans explication, elle risque toutefois de susciter la désapprobation générale, au risque d'être biffée du texte en vigueur.

Nous vous remercions de prendre bonne note de notre prise de position et restons à disposition pour tout complément d'information.

Pour la Commission fédérale de la Consommation

Prof. Dr. Pascal Pichonnaz
Président

Jean-Marc Vögele
Secrétariat

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

ETH-Bibliothek

ETH Zürich
Dr. Rafael Ball
Direktor ETH-Bibliothek
Rämistrasse 101
8092 Zürich

Telefon + 41 44 632 21 25
rafael.ball@library.ethz.ch
www.library.ethz.ch

Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
CH-3003 Bern
Per Mail:
jonas.amstutz@bj.admin.ch

Zürich, 14. Oktober 2021

Vernehmlassung zur
Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrte Herr Amstutz

Die ETH-Bibliothek nützt die Gelegenheit zur Stellungnahme im Rahmen des Vernehmlassungsverfahrens zur Verordnung zum Bundesgesetz über den Datenschutz wie folgt:

1.1

Für die Bibliotheken und deren Library Management Systeme (LMS) halte ich fest, dass diese Personendaten in Verbindung mit der registrierten Nutzung von Medien im Rahmen von Ausleihen keinesfalls unter die Bestimmungen von Art. 4 Ziff. 1 E-VDSG fallen können. Diese Feststellung gilt sowohl für die Bibliotheken also auch die LMS-Dienstleister als «Auftragsbearbeiter» im Sinn der Verordnung. Es handelt sich dabei nicht um «umfangreich bearbeitete besonders schützenswerte Personendaten» gemäss Art. 5 Bst.c nDSG und den Erläuterungen in der Botschaft des Bundesrates zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (17.059). Als besonders schützenswerte Personendaten werden dort aufgeführt: ethnische Herkunft, Rassenzugehörigkeit, Gesundheitsdaten, Intimsphäre, Sexualleben, Geschlechtsidentität, genetische und biometrische Daten.

1.2

Das Gesetz selber listet zum Terminus explizit die folgenden Inhalte auf: Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten, biometrische Daten, die eine natürliche Person eindeutig identifizieren, Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, Daten über Massnahmen der sozialen Hilfe. Diese Aufzählung ist abschliessend und nicht beispielhaft, weshalb die von Bibliotheken erhobenen Daten davon ausgeschlossen werden können. Ausgeliehene Medien können zwar Hinweise über die Interessen von Personen geben; es sind aber keine Daten die «Ansichten oder Tätigkeiten» dokumentieren, wie das im Gesetz spezifiziert wird. Darum können Ausleihdaten nicht als besonders schützenswerte Personendaten interpretiert werden.

1.3

Ebenso wenig sind die LMS-Datenbanken geeignet, «ein Profiling mit hohem Risiko» zu ermöglichen, wie das in den Materialien zum nDSG und zur E-VDSG erläutert wird. Dieses Verständnis ist von Bedeutung, weil damit die Pflicht von Art. 4 E-VDSG zur Erstellung eines Bearbeitungsreglements entfällt. Summa summarum fallen unter den beiden Aspekten «besonders schützenswerte Personendaten» sowie «Profiling mit hohem Risiko» die Bibliotheken und deren LMS-Daten bzw. ihre Auftragsbearbeiter nicht unter die Bestimmung von Artikel 4 der E-VDSG.

2.

Analog ist eine Pflicht der Bibliotheken gemäss Art. 26 E-VDSG zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten zu verneinen. Die beiden Buchstaben a und b sehen eine Ausdehnung auch auf Unternehmen und privatrechtliche Organisationen mit weniger als 250 Beschäftigten vor. Die genannten Voraussetzungen «umfangreich besonders schützenswerte Personendaten» oder «Profiling mit hohem Risiko» werden von LMS-Datenbanken gemäss den Ausführungen oben nicht erfüllt.

3.

Ich möchte sicherstellen, dass unsere Interpretation von nDSG und E-VDSG gemäss den vorstehenden Ausführungen zutrifft. Deshalb beantrage ich, dass die Verordnung in diesem Sinn ergänzt und verdeutlicht wird. Ich schlage vor, Art. 4 durch einen neuen Absatz 2 zu ergänzen und die weiteren Absätze entsprechen neu zu nummerieren:

4.

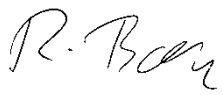
VDSG, Artikel 4, neuer Absatz 2: «Nicht unter die vorstehenden Buchstaben a und b fallen Daten, die von Bibliotheken, Mediotheken, vergleichbaren Einrichtungen und ihren Auftragsbearbeitern für Medienausleihen erhoben werden.»

5.

Die Nummerierung der folgenden Absätze ist entsprechend anzupassen.

Ich danke Ihnen für die Kenntnisnahme der Vernehmlassung und der entsprechenden Bearbeitung der künftigen Verordnung.

Mit freundlichen Grüssen



Dr. Rafael Ball
Direktor ETH-Bibliothek

EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Eidgenössisches Justiz- und Polizeidepartement EJPD
Karin Keller-Sutter
Bundeshaus West
3003 Bern

Zustellung per E-Mail an: jonas.amstutz@bj.admin.ch

Zürich, 14. Oktober 2021

Stellungnahme zum Verordnungsentwurf zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrte Frau Bundesrätin,
sehr geehrte Damen und Herren

Im Rahmen der laufenden Anhörung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG), welche am 23. Juni 2021 vom Bundesrat in die Vernehmlassung geschickt worden ist, möchten wir gerne die Gelegenheit nutzen, zur Vorlage Stellung zu nehmen.

I. Einleitung

EXPERTsuisse – der Schweizer Expertenverband für Wirtschaftsprüfung, Steuern und Treuhand – engagiert sich aktiv für seine rund 10'000 Einzelmitglieder und über 800 Mitgliedunternehmen (mit gut 19'000 Mitarbeitenden) sowie für einen starken Wirtschaftsstandort Schweiz. Die Mitgliedunternehmen von EXPERTsuisse betreuen den Grossteil der Schweizer Wirtschaft.

EXPERTsuisse setzt sich im Digitalisierungszeitalter für einen modernen, zeitgemässen Datenschutz ein, analog der DSGVO, damit Schweizer Recht international anerkannt und insbesondere seitens der EU als äquivalent eingestuft wird. Gleichzeit sollen Innovationen nicht behindert werden.

EXPERTsuisse hat im April 2017 eine Stellungnahme zum Vernehmlassungsentwurf des Bundesgesetzes über den Datenschutz (E-DSG) eingereicht und hatte bereits damals darauf hingewiesen, dass das neue Datenschutzrecht der Schweiz den Vorgaben auf EU-Ebene entsprechen muss, ohne über diese Vorgaben hinauszugehen.

II. Zusammenfassung

Mit der Zunahme digitaler Technologien sind auch die Anforderungen an den Datenschutz gestiegen. Das übergeordnete Ziel ist, die Persönlichkeit und die Freiheiten von Datensubjekten zu schützen. In Anbetracht der europäischen Entwicklungen musste auch die Schweiz ihr Datenschutzrecht revidieren. Dies einerseits, um den internationalen Erwartungen gemäss der künftigen revidierten Europaratskonvention 108 zu genügen und andererseits, um die für die Wirtschaft sehr wichtige Äquivalenz mit der EU-DSGVO zu bewahren. Eng damit verknüpft ist die ePrivacy-Verordnung, die ebenfalls von der EU verabschiedet wurde.

Der Beitritt zur modernisierten Datenschutzkonvention des Europarates hat für die Schweiz sowohl in Bezug auf den Schutz der Privatsphäre als auch für den internationalen Datenverkehr grosse Bedeutung. Die Revision wurde in der Herbstsession 2020 in der Schlussabstimmung angenommen, was den Weg frei macht für die Bewahrung der Anerkennung der Äquivalenz durch die EU. Der Äquivalenzentscheid durch die EU ist jedoch noch hängig.

Der E-VDSG enthält einige verschärfte Bestimmungen, für die gemäss Gesetz keine Grundlage besteht. Dadurch erscheint die Verordnung in gewissen Punkten wie ein Regelwerk mit materiell zusätzlichen Bestimmungen. Dies zeigt sich in dem Verordnungs-Entwurf als auch im Erläuterungsbericht.

Auf zu detaillierte Bestimmungen, die über das Niveau der DSGVO gehen, ist aus wirtschaftsliberaler Sicht zu verzichten. Der Entwurf muss unter der Berücksichtigung des revDSG und der politisch intensiv geführten Diskussionen unbedingt nachgebessert werden.

III. Vorschläge zur Überarbeitung der E-VDSG

In der heutigen digitalisierten Welt muss eine Balance gefunden werden zwischen angemessenem Datenschutz und der Wirtschaftlichkeit. Mit dem revDSG konnte ein modernes Gesetz geschaffen werden, das den aktuellen Anforderungen, mit Blick auf die internationale Ebene, gerecht wird. Insbesondere die Annäherung an die DSGVO der EU macht die Regulierung gut umsetzbar als auch kompatibel mit internationalen Normen.

In der E-VDSG sind zahlreiche Erweiterungen enthalten, die für die Wirtschaft, insbesondere für KMU, einen administrativen Mehraufwand bedeuten. Gewisse Regelungen, welche bereits im politischen Prozess bei der DSG-Revision abgelehnt wurden, wurden nun in der E-VDSG wieder aufgenommen. Zu erwähnen ist hier z.B. die in Art. 16 E-VDSG vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren (wurde vom Parlament gestrichen). Es ist zu vermuten, dass gerade KMU solche Anforderungen nur mit einem grossen Mehraufwand umsetzen können bzw. die Ressourcen dafür nicht zur Verfügung stehen (Konflikt mit Art. 60ff. revDSG - Strafbestimmungen).

Sinn und Zweck einer Ausführungsverordnung ist es, Gesetzesbestimmungen durch Details genauer zu beschreiben, so dass die Umsetzung des revDSG erleichtert werden sollte. Neue Normen dürfen jedoch nicht geschaffen werden.

Folgendes gilt es im Generellen zu beachten:

- Eine Überarbeitung und Verbindung zum revDSG erscheint zwingend notwendig zur Verhinderung von Swiss Finishes. Auf Einschränkungen, die nicht explizit auf Gesetzesstufe erwähnt sind und über das Niveau der DSGVO hinausgehen, ist zu verzichten. Verschärfungen im Vergleich zum EU-Standards bedeuten für die Wirtschaft zwei unterschiedliche Regelungen und Mehraufwände in der praktischen Umsetzung.
- Widersprüche zum revDSG sind grundsätzlich zu beheben und es wäre sinnvoll, bei einzelnen Verordnungsbestimmungen jeweils auf den Artikel der revDSG zu verweisen.
- Diskussionen, die im politischen Prozess zum revDSG bereits abgewiesen wurden, dürfen nicht auf dem Verordnungsweg wieder eingeführt werden.
- Aufgrund der kurzen Frist schlagen wir eine Übergangsfrist von 1 Jahr vor ab Inkrafttreten des revDSG. Es ist fragwürdig, ob die Wirtschaft ihre Compliance-Projekte rechtzeitig vorantreiben und abschliessen kann.

Konkrete (nicht abschliessende) Aspekte, die wir zur Überarbeitung vorschlagen:

- Grundsätze Art 1, Abs. 2 E-VDSG: Steigt das Risiko für die Rechte der Betroffenen, so soll die Prüfung der Massnahmen regelmässig stattfinden. Ab einem gewissen Risiko empfehlen wir, die Prüfung zu standardisieren (z.B. mittels ISO 27001 als Pflicht). Diese internationale Norm zeigt auf, dass eine Organisation Best-Practice-Prozesse zur Informationssicherheit definiert und umgesetzt hat.

- Schutzziele Art. 2 E-VDSG: Es ist nicht zwingend jedes dieser Schutzziele relevant, jedoch muss begründet werden können, warum nicht. Die Auflistung der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden. Dann wäre die Liste identisch mit Art. 32, Abs. 1 lit. b DSGVO.
- Protokollierung Art. 3 E-VDSG: Der gesamte Artikel soll ersatzlos gestrichen werden aufgrund der fehlenden gesetzlichen Grundlage. Im politischen Prozess hatte das Parlament bereits auf eine Protokollierungspflicht verzichtet.
- Art. 3, Abs. 1 E-VDSG: Das Ergebnis der DSFA ist kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. In den meisten Fällen wird eine DSFA nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenverarbeitung. Dies hat jedoch mit Datensicherheit nichts zu tun.
- Bearbeitungsreglement von privaten Personen: Art. 4 E-VDSG: Es fehlt eine gesetzliche Grundlage. Eine Einführung mittels Verordnung ist daher nicht möglich und es ist auch redundant, da die Informationen entweder in einer DSFA oder dann im Verzeichnis der Bearbeitungstätigkeiten enthalten sein werden.
- Modalitäten Art. 6, Abs 2 E-VDSG: Der Sinn und Zweck dieser Bestimmung erscheint unklar, da die Regelung bereits durch die Art. 16 und 17 revDSG abgedeckt ist (Bekanntgabe von Personendaten ins Ausland).
- Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internat. Organs: Art. 8, Abs 1, 3 E-VDSG braucht eine Präzisierung und könnte falsch verstanden werden. Der Bundesrat muss die Angemessenheit des Datenschutzes in einem Empfängerstaat feststellen (und nicht die verantwortliche Stelle).
- Datenschutzklauseln und spezifische Garantien Art 9. E-VDSG: Die gestellten Anforderungen erreichen ein Detailierungsgrad, der die Komplexität der Datenbearbeitung ineffizient gestaltet. Aus Sicht des Datenschutzes ist diese Regelung zur Erreichung des Datenschutzes zwar konsequent, doch verursacht hohe Aufwände für die Betriebe. Aus diesen Gründen empfehlen wir diese Anforderung auf das Minimum zu reduzieren.
- Verbindliche unternehmensinterne Datenschutzvorschriften Art. 11, Abs. 2: der Artikel geht weniger weit als Art. 47 DSGVO. Die bisherigen Binding Corporate Rules (BCR) wurden regelmässig so formuliert, dass diese auch EU-konform sind.
- Modalitäten der Informationspflichten: Art. 13 E-VDSG beschreibt, dass die Information über die Beschaffung von Personendaten in exakter, verständlicher und leicht zugänglicher Art kommuniziert werden soll. Werden Piktogramme verwendet, müssen diese maschinenlesbar sein. Letzteres soll gemäss dem Erläuterungsbericht einen Vergleich verschiedener Dokumente und allgemein eine gewisse Automatisierung ermöglichen. Es

stellt sich hier die Frage, wie weit dies ein Ziel des Datenschutzes ist. Wir stellen uns ausserdem die Frage, welches die gesetzliche Grundlage ist für diese Bestimmung. Art. 13 Abs. 1 E-VDSG sieht zudem vor, dass der Verantwortliche und der Auftragsbearbeiter die Information über die Beschaffung mitteilen. Das scheint dem Auftragsbearbeiter tatsächlich eine Informationspflicht gegenüber betroffenen Personen aufzuerlegen, was weder im Gesetz (Art. 19 revDSG) vorgesehen noch praktikabel ist. Es ist die Verantwortung des Verantwortlichen, betroffene Personen zu informieren und diese darf nicht auf dem Wege der Verordnung auf den Auftragsbearbeiter ausgedehnt werden. Das könnte auch in der Praxis zu Problemen führen. Zudem sollte man "mitteilen" umformulieren, es geht um die Informationspflicht (die passiv sein kann), nicht eine Mitteilungspflicht (die aktives Handeln min. impliziert).

- Für die «Information bei der Bekanntgabe von Personendaten» gemäss Art. 15 E-VDSG existiert keine gesetzliche Grundlage. Dies ist ein reiner Swiss Finish, der nach EU-Recht, zumindest für private Datenanbieter, nicht vorgeschrieben ist und wirkt und praxisfremd.
- Die in Art. 16 E-VDSG vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren, wurde vom Parlament bereits im Entwurf des revDSG gestrichen.
- Meldung von Verletzungen der Datensicherheit, Art. 19, Abs. 5: gemäss der DSGVO ist eine Dokumentation vorgesehen, nicht jedoch gemäss revDSG. Selbst die Botschaft zum revDSG sah keine Dokumentationspflicht vor**.** Eine Einführung mittels Verordnung ist daher nicht möglich.
- Modalitäten Art. 20, Abs. 5: Das revDSG sieht keine Dokumentation dieser Art vor. Eine Dokumentationspflicht ist aus diesem Grund zu streichen.
- Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten- Art. 26 E-VDSG: Die Voraussetzungen für die Ausnahme von der Befreiung von der Pflicht zur Führung eines Bearbeitungsverzeichnisses für KMU in Art. 26 E-VDSG ist unpräzis, insbesondere diejenige der "umfangreichen" Bearbeitung von besonders schützenswerten Personendaten. Da schwierig zu beurteilen ist was umfangreich bedeutet, kann dies unter Umständen auch bei KMU schnell vorliegen, insbesondere im Bereich der Bearbeitung von Personalinformationen. Ausserdem ist nicht klar, ob das Bearbeitungsverzeichnis dann nur für diese Bearbeitungen erstellt werden muss oder sich die Pflicht dann auf alle Bearbeitungen bezieht. Dies kann für KMU einen grossen Unterschied ausmachen. Die Anforderungen sind zu präzisieren und die Folgen der Pflicht klarzustellen.

Diese Vernehmlassung wurde in Abstimmung mit anderen Wirtschaftsverbänden erarbeitet. Wir gehen davon aus, dass im Anschluss an das Vernehmlassungsverfahren, das bis zum 14. Oktober dauert, noch Anpassungen der E-VDSG erfolgen werden.

Wie bereits erwähnt, erscheint uns die vorliegende Version als zu restriktiv (unnötige Swiss Finishes generieren keinen Mehrwert). Unternehmen, die bereits die DSGVO- Vorgaben eingeführt haben, werden keine Mühe bekunden bei der Umsetzung des revDSG.

Wir danken Ihnen für die Prüfung und Berücksichtigung unserer Anliegen. Für allfällige Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

EXPERTsuisse

Sergio Ceresola
Ressortleitung Regulatorisches & Fachliches
Mitglied der Geschäftsleitung

Markus Braun
Fachprojektleiter Governance & Regulation

Fédération des
Entreprises
Romandes

jonas.amstutz@bj.admin.ch

Madame Karin Keller-Sutter,
Conseillère fédérale

Département fédéral de justice et police
DFJP

Genève, le 11 octobre 2021
JD/3294 - FER No 32-2021

Projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Madame la Conseillère fédérale,

La Fédération des Entreprises Romandes (ci-après également « la FER »), qui représente plus de 45'000 entreprises en Suisse romande, se réfère à la procédure de consultation en lien avec la modification des ordonnances mentionnées en titre.

Notre Fédération vous prie de trouver ci-après sa prise de position y relative :

I. Remarques générales

Sur le principe, la FER ne s'oppose pas à la révision proposée, l'objectif de cette révision étant notamment de prendre en compte les rapides évolutions technologiques et les développements du droit européen.
En revanche, notre Fédération n'accepte pas certaines modifications proposées, notamment celles qui augmentent les coûts pour les entreprises de manière excessive et disproportionnée.
Par ailleurs, elle trouve regrettable que l'on ne puisse pas chiffrer les coûts de la révision de l'OLPD.

II. Commentaires article par article du projet de révision totale de OLPD (ci-après : P-OLPD)

Ad art. 4 al. 3 P-OLPD Règlement de traitement par des personnes privées

Pour reprendre les termes de l'art. 4 al. 1 P-OLPD, nous suggérons de remplacer le terme « la personne privée », par « le responsable du traitement ou son sous-traitant ».

Ad art. 6 al. 1 P-OLPD Sous-traitance

Selon l'art. 9 al. 2 nLPD : «Le responsable du traitement doit en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données».

L'art. 6 al. 1 P-OLPD prévoit que : «Le responsable du traitement qui confie un traitement de données personnelles à un sous-traitant demeure responsable de la protection des données. Il s'assure que les données soient traitées conformément au contrat ou à la loi».

Cette clause est inacceptable, car impraticable. Elle va trop loin, et ce tant par rapport à la loi que par rapport à l'art. 22 al. 3 de la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Quant à l'art. 28 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) (ci-après : RGPD), il ne mentionne pas non plus que le responsable du traitement qui confie un traitement de données personnelles à un sous-traitant demeure responsable de la protection des données.

Notre Fédération n'accepte donc pas l'art. 6 al. 1 P-OLPD.

Ad art. 8 al. 5 P-OLPD Communication des données personnelles à l'étranger

Selon l'art. 8 al. 5 P-OLPD et le Rapport explicatif[1], il est prévu que les Etats, pour lesquels un niveau de protection adéquat a été constaté par le Conseil fédéral (cf. art. 16 al. 1 nLPD), sont mentionnés en annexe à l'Ordonnance.

Selon le Rapport explicatif[2], il s'agit d'une liste « positive ». Si un Etat n'y figure pas, cela ne signifie pas nécessairement qu'il est dépourvu d'une législation sur la protection des données assurant un niveau de protection adéquat ; il est possible qu'il n'ait simplement pas fait l'objet d'un examen par le Conseil fédéral. Ce procédé diffère quelque peu du procédé actuel. En effet, actuellement, le PFPDT publie un document dans lequel il précise à côté de chaque Etat si celui-ci atteint un niveau adéquat pour les personnes physiques, un niveau adéquat sous certaines conditions ou un niveau insuffisant. Selon nous, le procédé actuel donne plus de sécurité juridique pour les entreprises et devrait être maintenu.

Ad art. 9 al. 1 let. e P-OLPD Clause de protection des données d'un contrat et garanties spécifiques

L'art. 9 al. 1 let. e P-OLPD mériterait d'être complété de la manière suivante :

«***Le cas échéant***, le nom des organismes internationaux de destination».

Ad art. 9 al. 1 let. k ch. 4 P-OLPD Clause de protection des données d'un contrat et garanties spécifiques

L'art. 9 al. 1 let. k ch. 4 devrait être biffé, car l'indépendance ou non d'une autorité de justice ne dépend pas du responsable de traitement.

---

[1] Rapport explicatif, p. 26

[2] Ibidem

Ad art. 10 al. 2 P-OLPD Clauses types de protection des données

Actuellement, l'art. 6 al. 5 OLPD prévoit que la décision du PFPDT est rendue dans un délai de 30 jours.
Or ce délai ne figure plus à l'art. 10 al. 2 P-OLPD.

Selon le Rapport explicatif[3], il faut se référer à l'art. 4 de l'Ordonnance du 25 mai 2011 sur les principes et les délais d'ordre relatifs aux procédures d'autorisations (OdelO), article qui prévoit que les délais peuvent être plus longs que 30 jours.

Nous sommes d'avis que le délai de 30 jours doit être maintenu et l'art. 10 al. 2 P-OLPD complété en ce sens.

Autrement dit, l'art. 10 al. 2 P-OLPD doit être complété comme suit « [...]. ***Il communique sa décision au responsable de traitement dans un délai de 30 jours à compter de la date de leur annonce*** ».

Ad art. 11 P-OLPD Règles d'entreprises contraignantes

Cet article appelle deux remarques de notre part.
Premièrement, l'art. 11 al. 2 let. a P-OLPD prévoit que les règles d'entreprises contraignantes pour les groupes de sociétés, règles qui doivent être soumises au PFPDT, doivent notamment porter sur la structure et les coordonnées du groupe d'entreprises et de chacune de ses entités.

Le fait de devoir communiquer sur la structure du groupe et les coordonnées du groupe d'entreprises et de chacune de ses entités ne résulte pas de la loi. L'art. 16 al. 2 let. e nLPD ne le prévoit pas. Cette exigence est excessive. La communication des mesures mises en place au sein des groupes d'entreprises pour garantir le contrôle du respect des règles d'entreprise contraignantes est suffisante (cf. art. 11 al. 2 let. b P-OLPD).

Deuxièmement, l'actuel art. 6 al. 5 OLPD prévoit que le préposé examine les garanties et les règles de protection des données qui lui sont annoncées (art. 31 al. 1 let. e LPD) et communique son résultat dans les 30 jours, sans obliger le maître du fichier à donner toutes les informations requises par l'art. 11 al. 2 let. a P-OLPD.

L'art. 11 P-OLPD ne fixe plus de délai au PFPDT pour communiquer son résultat. Le rapport explicatif renvoie à l'art. 4 de l'ordonnance du 25 mai 2011 sur les principes et les délais d'ordre relatifs aux procédures d'autorisations.

Selon nous, il faudrait conserver le libellé actuel de l'art. 6 al. 5 OLPD, car en supprimant le délai de 30 jours, le délai peut être plus long, comme le prévoit l'art. 4 OdelO.

Ad art. 6, 18 et 20 al. 1 et 2 P-OLPD

Ad art. 6, 18 et art. 20 al. 1 et 2 P-OLPD : ces dispositions prévoient la forme écrite, mais le Rapport explicatif précise que la forme écrite comprend la forme électronique (cf. pages 24, 31, 33 et 34).

A des fins de clarté et de sécurité juridique, nous pensons qu'il serait opportun de l'indiquer expressément dans le texte de l'ordonnance et non pas seulement dans le rapport explicatif.

---

[3] Rapport explicatif, p. 28

Ainsi l'art. 6 al. 3 P-OLPD devrait avoir la teneur suivante : «Lorsque le responsable de traitement est un organe fédéral, le sous-traitant ne peut sous-traiter le traitement des données à un tiers que si l'organe fédéral l'a approuvé par écrit ***ou sous forme électronique***.»
L'art. 18 P-OLPD devrait, quant à lui, être libellé comme suit : «Le responsable du traitement consigne par écrit ***ou sous format électronique*** l'analyse d'impact relative à la protection des données personnelles. […]».

L'art. 20 al. 1 P-OLPD devrait être complété comme suit : La demande de renseignement est faite par écrit ***ou sous format électronique***. […] Par ailleurs, la même modification devrait être faite dans toutes les ordonnances en annexe qui précisent que la demande d'accès doit être faites par écrit.

Enfin, le libellé de l'art. 20 al. 2 P-OLPD devrait être le suivant : «Les renseignements sont en principe fournis par écrit ***ou sous format électronique***. […]»

Ad 13 al. 2 P-OLPD

L'art. 13 al. 2 P-OLPD prévoit que : «Lorsque l'information se fait en combinaison de pictogrammes, ceux-ci doivent être lisibles par machine s'ils sont présentés par voie électronique».

Cette disposition mériterait d'être précisée, en particulier s'agissant des termes «lisibles par machine».
En outre, une reformulation de la première partie s'impose, dans le sens de la version de cet article en allemand (« *in Kombination mit* ») et du Rapport explicatif[4]. Le début de cette disposition pourrait par exemple être ainsi formulé : «Lorsque l'information ***est accompagnée*** de pictogrammes […]».

Ad art. 19 al. 3 P-OLPD Annonce des violations de la sécurité des données

L'art. 19 al. 3 P-OLPD prévoit que : «Le responsable du traitement communique à la personne concernée, dans un langage simple et compréhensible, au moins les informations visées à l'al. 1 let. a, e, f et g».

Le Rapport explicatif[5] précise que cette disposition s'applique si la personne concernée doit être informée conformément à la loi.

Le libellé de l'art. 19 al. 3 P-OLPD devrait donc être le suivant : «***Si la personne concernée doit être informée conformément à l'art. 24 nLPD, alors le responsable du traitement communique à la personne concernée, dans un langage simple et compréhensible, au moins les informations visées à l'al. 1 let. a, e, f et g***».

Ad art. 19 al. 5 P-OLPD Annonce des violations de la sécurité des données

L'art. 24 al. 2 nLPD prévoit que l'annonce doit indiquer au moins la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées.

L'art. 19 al. 5 P-OLPD prévoit notamment que le responsable du traitement documente les violations et que la documentation doit contenir tous les faits relatifs aux incidents et à leurs effets.

En pratique, nous ne comprenons pas comment le responsable du traitement peut deviner les effets qu'aura une violation dans le futur. Il ne peut qu'émettre des hypothèses.

---

[4] Rapport explicatif, p. 29
[5] Rapport explicatif, p. 32

Du reste l'art. 33 al. 3 let. c RGPD parle des «conséquences probables».

L'art. 19 al. 5 P-OLPD devrait donc être modifié comme suit : «Le responsable du traitement documente les violations. La documentation contient tous les faits relatifs aux incidents, à leurs ***conséquences possibles*** et aux mesures prises».

Ad art. 20 al. 5 P-OLPD Droit d'accès

L'art. 20 al. 5 P-OLPD prévoit que : *«Le responsable du traitement documente le motif pour lequel il refuse, restreint ou diffère la communication des informations. La documentation est conservée pendant au moins trois ans».*

La durée de conservation fixée à trois ans nous paraît excessive. Une durée de deux ans par analogie à la durée fixée, par l'Ordonnance du 22 novembre 2017 concernant la protection des données personnelles du personnel de la Confédération[6], pour la durée de conservation des procès-verbaux nous semblerait plus adéquate.

Ad art. 23 P-OLPD Exception à la gratuité

L'art. 23 al. 3 P-OLPD prévoit que la personne concernée est préalablement informée du montant et peut retirer sa requête dans les dix jours.

En tenant compte du fait que les renseignements doivent être fournis en principe dans les 30 jours suivant la réception de la demande (cf. art. 22 P-OLPD), le délai de 10 jours susmentionné paraît long et ne laisse plus beaucoup de temps pour transmettre, le cas échéant, les données.

L'art. 23 al. 3 P-OLPD devrait plutôt être libellé comme suit : «La personne concernée est préalablement informée du montant et peut retirer sa requête ***dans les 7 jours calendaires***».

Ad art. 27 P-OLPD Conseiller à la protection des données

L'art. 27 P-OLPD prévoit que : «Tout organe fédéral désigne un conseiller à la protection des données personnelles. Plusieurs organes fédéraux peuvent désigner conjointement un conseiller.»
Il ressort du Rapport explicatif[7] qu'un Office fédéral est un organe fédéral.

Or, désigner un conseiller par organe fédéral est une solution trop onéreuse et disproportionnée. A noter qu'actuellement, l'art. 23 OLPD prévoit un conseiller pour la Chancellerie et un conseiller pour chaque Département. Il y a sept Départements fédéraux, mais beaucoup plus d'Offices fédéraux.
La solution actuellement en vigueur à l'art. 23 OLPD nous paraît suffisante.

Rien ne justifie de la modifier, alors même que la définition d'«organe fédéral» dans la loi reste la même dans la nouvelle LPD (cf. art. 3 LPD et art. 5 nLPD).

L'art. 27 P-OLPD doit donc reprendre la teneur de l'art. 23 OLPD, à savoir : «La Chancellerie fédérale et chaque département désignent respectivement et au minimum un conseiller à la protection des données».

---

[6] RS 172.220.111.4

[7] Rapport explicatif, p. 39

Ad art. 44 P-OLPD Codes de conduite

L'art. 44 P-OLP prévoit que : «Si un code de conduite est soumis au PFPDT, celui-ci indique dans sa prise de position si le code de conduite remplit les conditions de l'art. 22, al. 5, let. a et b, LPD.»

D'une part, il est regrettable qu'il ne s'agisse pas d'une décision au sens formel, mais seulement une prise de position.

D'autre part, dans la mesure où le PFPDT facture un émolument pour rendre une prise de position, il serait opportun qu'un délai soit prévu pour rendre la prise de position, respectivement que ce délai ne soit pas trop long. Un délai de maximum 30 jours, par analogie à celui prévu par l'art. 6 al. 5 OLP, nous paraît opportun.

Ad art. 45 P-OLPD Emolument

L'art. 59 al. 2 nLPD prévoit que le Conseil fédéral fixe le montant des émoluments.

Or, le projet de l'art. 45 P-OLPD est libellé comme suit : «L'émolument perçu par le PDPDT se calcule en fonction du temps consacré. Il varie entre 150 et 350 francs l'heure. Il dépend de la complexité de l'affaire et de la fonction de la personne chargée de traiter le dossier ».

A noter que, par analogie, l'ordonnance sur les émoluments relatifs à l'octroi des permis concernant la durée du travail prévus par la loi sur le travail[8] prévoit des émoluments dont le montant est plafonné à CHF 400.

Plus précisément, l'art. 3 al. 1 et 2 de cette ordonnance relative au calcul de l'émolument indique ceci :

« Le SECO fixe le montant des émoluments en fonction du temps consacré.
Le tarif des émoluments est le suivant:

a. octroi d'un permis, le temps consacré étant de 3 h au plus	*200 fr.*
octroi d'un permis, le temps consacré étant supérieur à 3 h	*400 fr.*
b. modifications, par permis, le temps consacré étant de 3 h au plus	*50 fr.*
modifications, par permis, le temps consacré étant supérieur à 3 h	*100 fr.*

[2bis] Si la demande d'octroi d'un permis est transmise par voie électronique, le tarif des émoluments fixé à l'art. 2, let. a, est réduit de 25 %. »

Par analogie à l'ordonnance susmentionnée, l'art. 45 P-OLPD doit fixer des forfaits plafonnés.

Il n'est en effet pas acceptable que l'Etat puisse facturer des honoraires pour ses prestations de service public, dont le montant serait illimité.

Au vu de ce qui précède, l'art. 45 P-OLPD devrait être libellé comme suit : «L'émolument perçu par le PDPDT se calcule en fonction du temps consacré. Il varie entre 150 et 350 francs ~~l'heure~~. Il dépend de la complexité de l'affaire et de la fonction de la personne chargée de traiter le dossier».

Notre Fédération n'accepte donc pas la teneur de l'art. 45 P-OLPD, lequel devrait prévoir des émoluments sous forme de forfaits et non des honoraires calculés à l'heure.

---

[8] RS 822.117

III. Commentaires de l'Annexe 2 - Abrogation et modification d'autres actes

Ad art. 31 al. 1 de l'Ordonnance VIS du 18 décembre 2013[9]

Il manque le sujet à l'art. 31 al. 1. Nous proposons le libellé suivant : «Si une personne fait valoir son droit d'accès, son droit à la rectification ou son droit à l'effacement de données saisies dans ORBIS ou dans le C-VIS, ***elle*** présente une demande écrite au SEM. […]»

Ad art. 58 de l'Ordonnance du 16 janvier 1991 sur le service de l'emploi (ci-après : OSE)

L'art. 19 al. 2 let. c nLPD prévoit que lors de la collecte, le responsable de traitement communique à la personne concernée les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la présente loi et pour que la transparence des traitements soit garantie ; il communique au moins le cas échéant, les destinataires ou les *catégories de destinataires* auxquels des données personnelles sont transmises.

L'art. 58 al. 1 let. d OSE devrait reprendre le libellé de la loi. Plus précisément, il devrait être libellé comme suit : «Le cas échéant, des ***catégories de*** destinataires auxquelles des données sont transmises».

Quant à l'art. 58 al. 1 let. a, il doit être supprimé. Il n'y pas de base légale qui indique que l'identité et les coordonnées du responsable du système d'information doivent être communiquées. L'art. 19 al. 2 let. a nLPD ne mentionne que l'identité et les coordonnées du responsable du traitement.

Ad art. 126 de l'Ordonnance du 31 août 1983 sur l'assurance-chômage (ci-après : OACI)

Les remarques indiquées à l'art. 58 OSE valent également pour l'art. 126 OACI.

IV. Conclusion

En conclusion, la FER approuve sur le principe la révision proposée, avec les réserves susmentionnées.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre parfaite considération.

Blaise Matthey
Secrétaire général

Juliette Jaccard
Juriste

La Fédération des Entreprises Romandes en bref

Fondée le 30 juillet 1947 à Morat, son siège est à Genève. Elle réunit six associations patronales interprofessionnelles cantonales (GE, FR, NE, JU, VS), représentant la quasi-totalité des cantons romands. La FER comprend plus de 45'000 membres.

[9] RS 142.512

FMH

Eidgenössisches Justiz- und Polizeidepartement EJPD

Per E-Mail: jonas.amstutz@bj.admin.ch

Bern, 14. Oktober 2021

Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
Stellungnahme der FMH – Verbindung der Schweizer Ärztinnen und Ärzte

Sehr geehrte Frau Bundesrätin Keller-Suter

Sehr geehrte Damen und Herren

Die FMH nimmt zur vorgesehenen Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) gerne wie folgt Stellung:

Einleitende Bemerkungen
Grundsätzlich werden die Revisionsbestrebungen begrüsst, um einerseits die innerstaatlichen gesetzlichen Grundlagen den rasanten technologischen Entwicklung anzupassen und andererseits die Kompatibilität zu den neuen Rechtsgrundlagen des europäischen Datenschutzrechts zu gewährleisten. Der E-VDSG basiert auf zahlreichen Delegationsnormen im revDSG und konkretisiert Bestimmungen des revDSG, was zu begrüssen ist. Gleichzeitig enthält der E-VDSG Artikel, die von der bisherigen VDSG übernommen werden oder direkt an die DSGVO angelehnt sind, ohne sie aber inhaltlich

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

und terminologisch in den Gesamtentwurf einzupassen. Der E-VDSG verpasst es, diese Mindestanforderungen in einer Form zu konkretisieren, welche die heutigen Begrifflichkeiten und Anforderungen der Datensicherheit aufnehmen.

Für die Verantwortlichen ergibt sich ein unübersichtlicher Detaillierungsgrad, der die Umsetzung des revDSG nicht erleichtert. Was Fragen aufwirft, ist die unterschiedliche Handhabung der Termini, wie z.B. in Art. 4 «Bearbeitungsreglement» und in Art. 26 «Verzeichnis der Bearbeitungstätigkeiten», im Bewusstsein, dass diese Unterschiede auf die ursprünglichen Rechtsquellen (geltende VDSG und revDSG) zurückgehen. Es spricht aber nichts dagegen, hier eine einheitliche Terminologie zu verwenden.

Art. 8 Abs. 3 revDSG verlangt, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt. Der E-VDSG hält am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht. Aus den dargelegten Gründen vermag dieses Konzept nicht zu überzeugen.

Der bürokratische Aufwand, welcher mit der Umsetzung der vorliegenden Verordnung verbunden ist, entspricht zudem nicht dem Verhältnismässigkeitsprinzip. Hinzuweisen ist in diesem Kontext auf die Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung gemäss revDSG, die damit vorgegebenen Bearbeitungsreglemente von privaten Personen gemäss Art. 4 E-VDSG und schlussendlich die in Art. 3 E-VDSG verankerte Protokollierung, die an die Datenschutz-Folgenabschätzung anknüpft. Diese Umsetzung stellt an den Rechtsanwender grosse Herausforderungen und wird viel Aufwand generieren.

Schliesslich regen wir an, im Sinne der Rechtssicherheit die verschiedenen Aufbewahrungsfristen in der gesamten Verordnung zu vereinheitlichen. Es ist kein Grund ersichtlich, weshalb verschiedene Aufbewahrungsfristen in der vorliegenden Verordnung vorgesehen sind.

Zu den einzelnen Artikeln

Artikel	***Kommentar/Bemerkungen***	***Antrag für Änderungsvorschlag (Textvorschlag)***
Art. 1	Art. 1 E-VDSG übernimmt die Formulierung aus der DSGVO. Es wäre für die Umsetzung in der Praxis hilfreich, in Art. 1 Abs. 1 E-VDSG auch das übergeordnete Ziel der Massnahmen, ein dem Risiko angemessenes Schutzniveau zu erreichen, zu erwähnen. Des Weiteren ist darauf hinzuweisen, dass nicht nur die Implementierungskosten sondern der gesamte Implementierungsaufwand relevant ist.	Art. 1 Grundsätze [1] *Durch geeignete technische und organisatorische Massnahmen muss eine dem Risiko angemessene Datensicherheit gewährleistet werden.* Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung *einer* ~~der Datensicherheit~~ dem Risiko angemessenen *Datensicherheit geeignet* sind, beurteilt sich nach den folgenden Kriterien: a. Zweck, Art, Umfang und Umstände der Datenbearbeitung;

	Art. 1 Abs. 2 E-VDSG wäre sodann zu korrigieren: Nicht die Massnahmen sind laufend zu beurteilen, sondern die Risikobeurteilung.	b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen; c. der Stand der Technik; d. Implementierungs~~kosten~~*aufwand*. [2] Die *Risikobeurteilung* ~~Massnahmen sind~~ *ist* über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.
Art. 2	In Art. 2 E-VDSG sind die gängigen Schutzziele der Datensicherheit - Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit – in der heute üblichen Terminologie zu konkretisieren. Diese würde es den Verantwortlichen, z.B. den Arztpraxen, erleichtern, die Anforderungen in Zusammenarbeit mit den Informatikpartnern umzusetzen.	
Art. 3	Was heisst für den Rechtsanwender «*ergibt sich aus der Datenschutz-Folgenabschätzung….noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht*»? Diesbezüglich gibt es Rechtsunsicherheiten, die zu Lasten des Rechtsanwenders gehen. Ist eine Protokollierungspflicht im konkreten Fall auch dann gegeben, wenn die Datenschutz-Folgenabschätzung nicht durchgeführt wurde? Dies geht aus dem Verordnungsentwurf nicht hervor. Soweit eine Protokollierung gemäss Art. 3 Abs. 4 E-VDSG notwendig ist, erscheint eine Aufbewahrungsfrist von zwei Jahren unverhältnismässig. Zwei Jahre sollte eine Maximalfrist sein. Bei Abs. 4 muss der Grundsatz der Verhältnismässigkeit und der Datensicherheit gegeben sein.	
Art. 4	Das Bearbeitungsreglement von privaten Personen wird in der Praxis einen hohen Aufwand generieren.	

	Zudem ist zu definieren, was unter «umfangreich besonders schützenswerte Personendaten bearbeiten» versteht. Diesbezüglich sind Rechtsunsicherheiten für den einzelnen Rechtsanwender gegeben. Insbesondere kann es nicht sein, dass der Arzt in der Arztpraxis als Entscheidungsträger mit derartigen Rechtsunsicherheiten konfrontiert wird.	
Art. 6	Wichtige Präzisierung insbesondere was die haftpflichtrechtliche Verantwortlichkeit betrifft. Die Sicherstellungspflicht des Verantwortlichen entspricht nicht dem Verhältnismässigkeitsprinzip des Datenschutzrechts (siehe Art. 9 Abs. 2 revDSG: Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.). Der Verordnungswortlaut ist inhaltlich dem Gesetzeswortlaut anzupassen.	
Art. 13	In Art. 13 Abs. 1 ist der «Auftragsbearbeiter» und das Wort «und» zu streichen, denn gemäss revDSG hat der Auftragsbearbeiter eine Weisungsgebundenheit. Der Auftragsbearbeiter darf gemäss Art. 9 Abs. 3 revDSG die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.	
Art. 15	Auch hier wird der «Auftragsbearbeiter» wie in Art. 13 Abs. 1 zitiert. Der «Auftragsbearbeiter» ist zu streichen.	
Art. 16	Mit Bezug auf Art. 19 DSGVO liegt die Schlussfolgerung nahe, dass hiermit in casu ein Nachvollzug der DSGVO gegeben ist, obwohl sich die Pflicht, Empfängerinnen und Empfänger über «die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten» unverzüglich zu informieren, nicht im revDSG findet. «Unverzüglich» ist zudem in der Praxis nicht umsetzbar und auch in der DSGVO nicht vorgesehen.	Streichen

Art. 18	Es wäre zu erwarten, dass in der vorliegenden Verordnung diesbezüglich die Präzisierungen des Wortlautes revDSG Art. 22 Abs. 1 lit. a. «bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten» erfolgen sollten. Was heisst «umfangreiche Bearbeitung»? Es kann nicht sein, dass der Arzt in der Arztpraxis als Entscheidungsträger mit derartigen Rechtsunsicherheiten konfrontiert wird.	
Art. 19	Hier fehlt die Präzisierung des Art. 24 revDSG des Wortlautes «voraussichtlich». Was versteht man unter «voraussichtlich»? Es handelt sich um ein Adjektiv, welches für den Rechtsanwender nicht umsetzbar ist. Die Dauer von 3 Jahren erscheint willkürlich gewählt. Im Sinne der Vereinheitlichung sind hier 2 Jahre vorzusehen.	
Art. 20	Im erläuternden Bericht heisst es «Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen» (S. 35). Es kann nicht sein, dass die «Einsichtnahme an Ort und Stelle» eine Bedingung ist, um eine Fotokopie verlangen zu können. Ebenso ist hier angezeigt im Sinne der Vereinheitlichung für die Dokumentation die Frist von 2 Jahren vorzusehen.	
Art. 21 Abs. 1	Der Verordnungsentwurf sieht vor, wenn ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig ist, er dieses an den zuständigen Verantwortlichen weiterleitet. Hier erachten wir eine Präzisierung als notwendig, dass der Patient einerseits in Ausübung seines Selbstbestimmungsrechtes aber auch wegen dem vom Arzt zu wahrenden Arztgeheimnisses sagen muss, wer der zuständige Verantwortliche ist.	Art. 21 Abs. 1 E-VDSG soll wie folgt ergänzt werden: [1] Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter. *Die betroffene Person bezeichnet den zuständigen Verantwortlichen.*
Art. 26	Auch hier bedarf es der Ausführung was man unter «umfangreich besonders schützenswerte Personendaten» versteht. Nur dann können Unternehmen und andere privatrechtliche Organisationen subsumieren, ob sie unter diese Bestimmung fallen.	

Wir danken Ihnen im Voraus für die Berücksichtigung unserer Eingabe.

Freundliche Grüsse

Yvonne Gilli
Präsidentin

Nicole Furgler
Generalsekretärin ad interim

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Forum PME
KMU-Forum
Forum PMI

CH-3003 Berne, Forum PME

Par courriel

jonas.amstutz@bj.admin.ch
Office fédéral de la justice
Bundesrain 20
3003 Berne

Spécialiste: mup
Berne, 08.10.2021

Projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données

Madame, Monsieur,

Notre commission extraparlementaire s'est penchée, lors de sa séance du 2 septembre 2021, sur le projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD). Nous remercions Mmes Monique Cossali, Fanny Matthey et Daniela Nüesch de votre office d'avoir participé à cette séance et d'y avoir présenté les aspects du projet qui intéressent plus particulièrement les PME.

Les membres de notre commission sont de l'avis qu'aucune nouvelle obligation ne devrait être introduite dans l'OLPD révisée, si elle n'a pas de fondement dans la nouvelle loi adoptée par le Parlement le 25 septembre 2020 et si elle n'est pas absolument nécessaire en vue de garantir le maintien par l'Union européenne (UE) de sa décision de reconnaissance de l'adéquation de notre réglementation dans ce domaine. Sans décision positive de l'UE et sans libre circulation des données, nos entreprises – en particulier les PME concernées – subiront une importante perte de compétitivité. Nous sommes cependant opposés à tout « Swiss finish » qui aurait pour conséquence une augmentation des charges administratives et coûts pour les entreprises suisses, auxquels les entreprises européennes ne sont pas confrontées.

Nous demandons que les dispositions du projet d'OLPD révisée, en particulier celles qui concernent les obligations de documentation et d'information, soient revues et allégées. Certaines des dispositions proposées vont plus loin que la réglementation européenne et ont pour certaines été écartées lors du processus législatif. Nous sommes opposés à leur intégration à ce stade car elles créeraient des obligations allant au-delà de la volonté du Parlement. Cela concerne, entre autres, l'article 4 relatif au règlement de traitement des personnes privées ainsi que les articles 15 et 16 concernant les informations à fournir lors de la communication des données personnelles et leur rectification.

Forum PME
Holzikofenweg 36, 3003 Berne
Tél. +41 58 464 72 32
kmu-forum-pme@seco.admin.ch
www.forum-pme.ch

Le projet mis en consultation est, avec les nombreuses adaptations prévues d'autres ordonnances, très vaste. Pour un profane, il est difficile d'en appréhender tous les enjeux, même après un examen approfondi des différents articles et du rapport explicatif. Nombre de dispositions sont par ailleurs sujettes à interprétation. Nous demandons pour cette raison que le Conseil fédéral édicte des dispositions sur les exigences minimales, entre autres en matière de sécurité des données, comme cela est requis par l'article 8, al. 3 de la loi révisée. L'article 2 du projet d'ordonnance ne remplit pas complètement, à notre avis, le mandat adressé par cette disposition.

Nous estimons qu'il est en outre nécessaire que votre office et/ou le Préposé fédéral à la protection des données et à la transparence (PFPDT), prépariez des aides à l'application pour les entreprises, en particulier pour les PME. Il sera sinon compliqué, voire impossible pour nombre d'entre elles, de comprendre sur la base de la documentation mise en consultation, quels sont concrètement dans la pratique leurs devoirs dans ce domaine complexe. Des aides à la mise en œuvre sont pour cette raison absolument nécessaires. Elles devront permettre aux entreprises concernées de ne pas perdre inutilement de temps et de ne pas devoir nécessairement solliciter les services payants de consultants. Nous vous prions de publier sur vos pages Internet et/ou celles du PFPDT, au minimum six mois avant l'entrée en vigueur des nouvelles dispositions, toutes les informations susceptibles de simplifier la tâche des PME en vue de la mise en œuvre de la nouvelle réglementation.

Espérant que nos recommandations seront prises en compte, nous vous prions d'agréer, Madame, Monsieur, nos meilleures salutations. Nous nous tenons volontiers à votre disposition pour toute question éventuelle.

Jean-François Rime
Co-Président du Forum PME
Industriel, représentant de l'Union suisse des arts et métiers

Dr. Eric Jakob
Co-Président du Forum PME
Ambassadeur, Chef de la promotion économique du Secrétariat d'Etat à l'économie

Copie à : Préposé fédéral à la protection des données et à la transparence

FÉDÉRATION ROMANDE DES CONSOMMATEURS
LE POUVOIR D'AGIR

Département fédéral de justice
et police
Office fédéral de la justice

Envoyé par mail à
jonas.amstutz@bj.admin.ch

Lausanne, le 6 octobre 2021

Consultation sur la révision totale de l'ordonnance relative à la Loi fédérale sur la protection des données (OLPD)

Monsieur,

La Fédération romande des consommateurs (FRC) vous remercie de l'avoir associée à la consultation sur la révision totale de l'ordonnance relative à la Loi fédérale sur la protection des données (OLPD).

Les consommateurs de Suisse sont au centre des problématiques liées à la protection des données. L'asymétrie informationnelle, l'opacité des pratiques de collecte et d'exploitation des données personnelles, les incertitudes liées aux modalités de stockage de même que les risques de piratage rendent ces dispositions légales cruciales.

Notre association a activement pris part aux débats concernant la révision de la Loi sur la protection des données et, malgré certaines améliorations, regrette que les pouvoirs du Préposé fédéral n'aient pas été davantage renforcés, que les sanctions restent dérisoires et que la problématique du profilage à des fins de solvabilité n'ait pas été réglée[1].

Vous trouverez ci-après nos remarques en lien avec les points qui touchent directement les consommateurs.

[1] https://www.frc.ch/protection-des-donnees-lavenir-seclaircit-un-peu/

Fédération romande des consommateurs
Rue de Genève 17, Case postale 6151
1002 Lausanne
Tél. 021 331 00 90
info@frc.ch, www.frc.ch

Personne de contact
Marine Stücklin
Responsable Droit et Politique
m.stuecklin@frc.ch

Exigences minimales en matière sécurité des données (art. 8ss nLPD; art. 1ss P-OLPD)
Selon le nouvel article 61, let. c nLPD, celui qui ne respecte pas, intentionnellement, les exigences minimales en matière de sécurité des données édictées par le Conseil fédéral s'expose à une amende de 250 000 francs au plus (art. 61, let. c nLPD). Il est essentiel que le Conseil fédéral ne vide pas cette disposition de sa portée en prévoyant des mesures trop modestes ou trop peu claires.

En l'état, le projet ne permet pas de déterminer avec suffisamment de précision ce qui entrainerait l'application de la disposition pénale. En effet, l'utilisation de notions juridiques indéterminées dans cette section 1 est très regrettable car elle affaiblit l'étendue de la protection ainsi que la possibilité de recourir à la disposition pénale («A des intervalles appropriés», art. 1, al. 2 P-OLPD ; «Dans la mesure du possible», art. 2 P-OLPD); il convient d'y renoncer. La fréquence à laquelle les mesures doivent être réexaminées doit également être clairement indiquée dans l'ordonnance (art. 1 , al. 2 P-OLPD), toute marge d'interprétation et d'appréciation dans ce domaine risquant de porter atteinte à la sécurité des données.

Journalisation (art. 3 P-OLPD)
La journalisation doit permettre de vérifier le traitement des données personnelles *a posteriori*, afin de déterminer si des données ont été perdues, effacées, détruites, modifiées ou si elles ont été divulguées. Cette obligation joue donc un grand rôle en matière de sécurité. Néanmoins, la journalisation implique de fournir des informations sur la nature du traitement, l'identité de la personne qui a effectué le traitement, l'identité du destinataire et le moment auquel le traitement a eu lieu, etc. Elle peut donc représenter un risque de surveillance des personnes concernées, lequel est justifiable si le traitement envisagé présente un risque élevé pour la personnalité ou les droits fondamentaux. Aussi, le fait que la journalisation ne doit être effectuée que de manière subsidiaire, après une pesée des intérêts, devrait davantage ressortir du texte de l'art. 3 P-OLPD.

La journalisation ne devrait au surplus pas dépendre strictement des résultats de l'analyse d'impact. En effet, le responsable du traitement peut être délié de son obligation d'établir une analyse d'impact s'il soumet un code de conduite au PFPDT (art. 22, al. 5 nLPD) mais n'est pas forcé de le modifier s'il donne lieu à une prise de position critique du PFPDT (art. 11, al. 2 nLPD). Il en découle que tous les cas où les traitements envisagés présentent un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées doivent faire l'objet d'une journalisation, indépendamment de la tenue ou non d'une analyse d'impact.

Communication de données personnelles à l'étranger (art. 16ss nLPD; art. 8ss P-OLPD)
L'art. 8, al. 1 P-OLPD pose les critères qui doivent être pris en compte pour évaluer l'adéquation du niveau de protection de l'Etat de destination. Parmi les conditions figure le respect des droits humains (art. 8, al. 1, let. b P-OLPD). Bien que louable, ce critère ne semble pas suffisamment clair en tant que tel pour être pertinent. Il conviendrait de préciser que la garantie d'un procès équitable est un critère important, afin d'assurer à la personne concernée dont les données pourraient être utilisées à l'étranger, une défense équitable.

De manière générale, la possibilité d'octroyer une autorisation lorsqu'un secteur déterminé d'un Etat accorde un niveau de protection suffisant doit être conditionné au fait que le secteur déterminé n'est pas assujetti aux lois ou à certaines des lois de l'Etat dans lequel il se trouve. De même, seuls les territoires disposant d'une autonomie légale du point de vue de la protection des données devraient être éligibles. Ces critères devraient figurer dans l'ordonnance.

En l'absence de décision du Conseil fédéral, l'art. 16, al. 2 nLPD prévoit que les données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti notamment par un contrat conclu entre le responsable du traitement ou le sous-traitant et son cocontractant. Le PFPDT est informé. Dans ces cas et malgré les clauses de protection de données impératives listées à l'art. 9, al. 1 P-OLPD, nous jugeons grand le risque que ledit contrat et partant, le niveau de protection des données, ne soient jamais respecté dans certains pays.

De plus, au vu de l'expérience du « Swiss-U.S. Safe Harbor Framework », remplacé par le « Swiss-U.S. Privacy Shield Framework », lui-même ensuite révoqué, il semble illusoire de considérer qu'une telle entente puisse offrir une protection suffisante vis-à-vis de la primauté de l'intérêt d'Etat dans de nombreux pays.

Enfin, il nous paraît important de repréciser dans l'ordonnance que la communication de données à l'étranger doit respecter le niveau de protection de la nLPD.

Devoir d'informer (art. 19ss nLPD; 13ss P-OLPD)
Nous saluons les articles 13, al. 1 et 15 P-OLPD, lesquels précisent que les informations sur la collecte des données personnelles doivent être communiquées de manière concises, compréhensible et facilement accessibles et que les données personnelles communiquées sont actuelles, fiables et exhaustives. Ce n'est que de cette manière qu'une personne pourra se déterminer sur ses données et exercer ses droits.

Il est également essentiel que la personne concernée soit informée sans délai de la rectification, de l'effacement ou de la destruction de ses données pour s'assurer que ses instructions ont bien été suivies d'effet (art. 16 P-OLPD).

Décision automatisée (art. 21 nLPD; art. 17 P-OLPD)
Les décisions automatisées peuvent être injustes et une personne qui demande la réévaluation de sa demande par une personne physique ne doit pas être désavantagée pour ces motifs. Notre association salue donc cette disposition.

Droit d'accès (art. 25ss nLPD; 20ss P-OLPD)
Le droit d'accès figure parmi les droits les plus importants de la personne concernée et il est important de veiller à ce que son exercice ne soit pas rendu inutilement compliqué. A cet égard, une demande envoyée par mail avec preuve de l'identité doit pouvoir suffire.

La FRC salue en particulier l'art. 21 P-OLPD qui permet à la personne concernée d'adresser sa demande auprès de chaque responsable du traitement sans avoir à rechercher la personne compétente. Le délai de traitement d'une demande d'accès ne doit, dans tous les cas, pas excéder un délai de 30 jours (art. 22, al. 1 P-OLPD).

Concernant les exceptions à la gratuité (art. 23, P-OLPD), le fait de demander une participation équitable aux frais ne doit pas devenir un moyen pour les responsables de traitement de dissuader les personnes concernées d'avoir accès à leurs données. Pour cette raison, il convient d'ajouter «A titre exceptionnel» au début de l'alinéa 1 pour souligner le fait qu'une participation financière ne peut être demandée que dans de rares cas. Par ailleurs, le responsable du traitement, en plus de chiffrer le coût extraordinaire, devrait expliquer ce qui les justifie. En d'autres termes, il doit indiquer en quoi la demande occasionne des efforts disproportionnés. Dans la mesure où leurs obligations légales sont connues, les responsables du traitement

doivent s'organiser en amont pour qu'une demande d'accès soit facilement réalisable et que lesdits «efforts disproportionnés» restent rares.

Enfin, le responsable du traitement doit obtenir une confirmation de la part de la personne concernée avant de continuer à traiter sa demande, une absence de réaction ne devant en aucun cas pouvoir être interprétée comme un consentement aux frais (art. 23, al. 3 P-OLPD). L'obtention d'une confirmation écrite permettra par ailleurs d'éviter un travail inutile du responsable du traitement.

Exception à l'obligation de tenir un registre des activités de traitement (art. 12, al. 5 nLPD; art. 26 P-OLPD)
Notre association regrette beaucoup que les entreprises de moins de 250 employés (c'est-à-dire plus de 99% des entreprises en Suisses[2]) soient exemptées de l'obligation de tenir un registre des activités de traitement. Alors même que la protection des données constitue un enjeu majeur pour les PME qui traitent un volume de données personnelles toujours plus important et sont, conséquemment, parmi les cibles privilégiées des hackers. La tenue d'un registre constitue ainsi est un moyen simple pour permettre au responsable du traitement de s'assurer qu'il respecte bien ses obligations en matière de protection des données.

Le fait de vouloir limiter cette exception est bienvenu mais risque d'être vidé de toute portée si les notions de «données sensibles à grande échelle» et de «profilage à risque élevé» ne sont pas mieux définies (art. 26 P-OLPD). On se demande même si le fait de traiter de données sensibles ne devrait pas, en soi, constituer une telle exception sans qu'il soit nécessaire d'être face à un traitement « à grande échelle ».

Notions qui mériteraient un développement
De manière plus générale, on s'étonne que la ***notion de profilage à risque élevé*** (art. 5, let. g nLPD) ne soit pas davantage développée dans l'ordonnance dans la mesure où il s'agit d'une notion nouvelle, élaborée ex nihilo et ayant fait l'objet d'un large débat entre les deux Conseils. Il en va de même pour le concept de ***protection des données dès la conception et par défaut*** (art. 7 nLPD) qui ne fait l'objet d'aucune précision. Il conviendrait de mieux le définir, comme le fait le Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données dans son paragraphe introductif §78.

En vous remerciant de prendre en compte notre position, nous vous prions de recevoir, Monsieur, nos salutations les meilleures.

Fédération romande des consommateurs

Sophie Michaud Gigon
Secrétaire générale

Marine Stücklin
Responsable Droit et Politique

[2] https://www.bfs.admin.ch/bfs/fr/home/statistiques/industrie-services/entreprises-emplois/structure-economie-entreprises/pme.html

GASTROSUISSE

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail an:
jonas.amstutz@bj.admin.ch

Zürich, 14. Oktober 2021

Vernehmlassungsantwort

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

GastroSuisse, der grösste Branchenverband der Schweiz mit rund 20'000 Mitgliedern (Hotels, Restaurants, Cafés, Bars etc.) in allen Landesgegenden, organisiert in 26 Kantonalsektionen und vier Fachgruppen, nimmt im obengenannten Vernehmlassungsverfahren gerne wie folgt Stellung:

I. Allgemeine Würdigung

GastroSuisse befürwortet grundsätzlich die Bestrebungen, die Datenschutzbestimmungen mit der fortschreitenden Digitalisierung abzustimmen. Allerdings stellt der Branchenverband mit Besorgnis fest, dass die Verordnung teils über das Datenschutzgesetz als Rechtsgrundlage hinausgeht.

Die aus Sicht des Branchenverbands wichtigsten Änderungsvorschläge sind nachfolgend aufgeführt. Des Weiteren teilt GastroSuisse die im Rahmen der Vernehmlassung eingereichten Anliegen des Schweizerischen Gewerbeverbandes sgv.

II. Änderungsvorschläge

Art. 2 Schutzziele

Der Wortlaut soll wie folgt angepasst werden: «Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele *anstreben*:». Da es keine absolute Datensicherheit gibt, sollen Schutzziele angestrebt und nicht Mindeststandards erreicht werden.

Art. 6 Modalitäten

Gemäss Art. 9 Abs. 2 DSG muss sich die verantwortliche Person zwar vergewissern, dass die Datenbearbeitung durch einen Auftragsbearbeiter korrekt erfolgen kann. Allerdings soll die verantwortliche Person die korrekte Bearbeitung durch den Auftragsbearbeiter nicht *sicherstellen müssen*.

Art. 13 Modalitäten der Informationspflicht

In den Erläuterungen zu Art. 13 ist vermerkt, dass die betroffene Person «stets auf der ersten Kommunikationsstufe» informiert wird. Dies stellt im Vergleich zur Wortwahl «angemessen» gemäss Art. 19 DSG eine Verschärfung dar, da dies je nach Kommunikationsmittel nicht möglich ist. Der Branchenverband befürwortet eine entsprechende Präzisierung in den Erläuterungen.

Art. 23 Ausnahmen von der Kostenlosigkeit

Das Verhältnis zwischen möglichen Aufwandskosten und maximaler Beteiligung ist mit CHF 300.- unausgewogen. Der Höchstbetrag ist entsprechend anzuheben oder im Verhältnis zu den durch die Auskunft verursachten Kosten zu gestalten.

GastroSuisse
Für Hotellerie und Restauration
Pour l'Hôtellerie et la Restauration
Per l'Albergheria e la Ristorazione

Wirtschaftspolitik
Blumenfeldstrasse 20 | 8046 Zürich
T 0848 377 111
wipo@gastrosuisse.ch | www.gastrosuisse.ch

Art. 45 Gebühren

Der EDÖB arbeitet im Interesse der Gesellschaft. Personen, die sich an das EDÖB wenden, um sich datenschutzkonform zu verhalten, sollten nicht zusätzlich Gebühren in derartiger Höhe bezahlen müssen. Ferner erachten wir es grundsätzlich als nicht angemessen, wenn die Kosten in diesem Fall gemäss Aufwand berechnet werden. In der Regel haben die Personen, die sich an das EDÖB wenden, weder Einfluss auf die Komplexität der Problematik, noch Einfluss auf die Effizienz der EDÖB-Mitarbeitenden.

III. Ausnahme für KMU

GastroSuisse begrüsst ausdrücklich die Ausnahme für Unternehmen bis 250 Mitarbeitenden von der Pflicht, ein Verzeichnis der Bearbeitungstätigkeiten zu führen (Art. 26). Für kleine und mittlere Unternehmen wäre der administrative Aufwand andernfalls enorm und kaum tragbar.

IV. Übergangsfristen

Weder im neuen Datenschutzgesetz noch im vorliegenden Verordnungsentwurf sind Übergangsfristen zur Umsetzung definiert. Da das Inkrafttreten neue, weitgehende Verpflichtungen für Unternehmen beinhaltet, befürwortet GastroSuisse eine entsprechende Ergänzung in der Verordnung. Als Übergangsfrist schlägt der Branchenverband mindestens ein Jahr vor.

Wir danken Ihnen für die Berücksichtigung der Haltung von GastroSuisse.

Freundliche Grüsse

Casimir Platzer
Präsident

Daniel Borner
Direktor

GastroSuisse
Für Hotellerie und Restauration
Pour l'Hôtellerie et la Restauration
Per l'Albergheria e la Ristorazione

Wirtschaftspolitik
Blumenfeldstrasse 20 | 8046 Zürich
T 0848 377 111
wipo@gastrosuisse.ch | www.gastrosuisse.ch

DIE SPITÄLER DER SCHWEIZ
LES HÔPITAUX DE SUISSE
GLI OSPEDALI SVIZZERI

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz
Bundesrain 20
CH-3003 Bern

Per Mail an: jonas.amstutz@bj.admin.ch

Ort, Datum	Bern, 14. Oktober 2021	Direktwahl	031 335 11 59
Ansprechpartnerin	Cheryl von Arx	E-Mail	cheryl.vonarx@hplus.ch

Revision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG): Vernehmlassung
Stellungnahme H+

Sehr geehrte Frau Bundesrätin Keller-Suter
Sehr geehrte Damen und Herren

An seiner Sitzung vom 23. Juni 2021 hat der Bundesrat das Vernehmlassungsverfahren zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) eröffnet. H+ bedankt sich für die Möglichkeit zur Stellungnahme. Gerne lassen wir Ihnen unsere Stellungnahme hiermit fristgerecht zugehen.

H+ Die Spitäler der Schweiz ist der nationale Verband der öffentlichen und privaten schweizerischen Spitäler, Kliniken und Pflegeinstitutionen. Uns sind 208 Spitäler, Kliniken und Pflegeinstitutionen als Aktivmitglieder an 343 Standorten sowie über 150 Verbände, Behörden, Institutionen, Firmen und Einzelpersonen als Partnerschaftsmitglieder angeschlossen. Wir vertreten über 200‘000 Arbeitsverhältnisse.

Inhaltsverzeichnis der Stellungnahme

1. Einleitung

In der Herbstsession 2020 hat das Parlament das neue Datenschutzgesetz (nDSG) verabschiedet. Die Referendumsfrist lief im Januar 2021 unbenutzt ab. Damit dieses in Kraft treten kann, müssen die entsprechenden Ausführungsbestimmungen in der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) angepasst werden.
Der E-VDSG basiert auf zahlreichen Delegationsnormen im revDSG und konkretisiert Bestimmungen des revDSG. Der vorliegende Entwurf zur Revision der Verordnung zum Bundesgesetz über den Datenschutz (Datenschutzverordnung, VDSG) verfolgt auf Basis des totalrevidierten Datenschutzgesetzes (nDSG) folgende Ziele: die Verbesserung der Transparenz bei der Datenbeschaffung- und verarbeitung sowie die Stärkung der Selbstbestimmung der betroffenen Personen über ihre Daten. Gleichzeitig soll die Totalrevision der Schweiz erlauben, das revidierte Datenschutzübereinkommen SEV 108 des Europarats zu ratifizieren sowie die Schengen-relevante Richtlinie (EU) 2016/680 über den Datenschutz in Strafsachen umzusetzen. Die vorgesehenen Änderungen der vorliegenden Ausführungsbestimmungen betreffen etwa die Bestimmungen über die Mindestanforderungen an die Datensicherheit, die Modalitäten der Informationspflichten und des Auskunftsrechts oder die Meldung von Verletzungen der Datensicherheit.

Grundsätzlich begrüsst H+ die Neuerungen, die das Datenschutzrecht den veränderten technologischen und gesellschaftlichen Verhältnissen anpasst und andererseits die Kompatibilität zu den neuen Rechtsgrundlagen des europäischen Datenschutzrechts sicherstellt. H+ musste gleichzeitig feststellen, dass der E-VDSG zahlreiche Bestimmungen enthält, welchen eine gesetzliche Grundlage fehlt, oder dass sie gar dem Willen des Gesetzgebers widersprechen.

> *«Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus (Art. 164 Abs. 2 BV). Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen (Art. 182 Abs. 2 BV). Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck.» (BGE 141 II 169, E. 3.3).*

Die Verwaltung überdehnt ihre rechtsetzerische Kompetenz, indem sie auf dem Verordnungsweg unter dem Titel der Datensicherheit massgeblich die ganze Datenschutz-Governance als solche über das DSG hinaus auszubauen versucht. Damit ist die E-VDSG oft unnötig restriktiv. Sie würde zu einem massiven Mehraufwand für die Spitäler führen und bspw. auch die, notabene gesetzlich verankerte Pflicht, zur Sicherung, Verbesserung und Weiterentwicklung der Qualität von medizinischen Behandlungen unnötig weiter erschweren[1]. H+ billigt ein solches Vorgehen nicht. Es zeugt von wenig Gespür gegenüber dem politischen Prozess, wenn Regelungen in einer unselbstständigen Verordnung Eingang finden, die wohl formellgesetzlich zu regeln wären.

Zudem wurden Artikel von der bisherigen VDSG übernommen oder sind direkt an die DSGVO angelehnt, ohne sie aber inhaltlich und terminologisch in den Gesamtentwurf einzupassen.

Der E-VDSG verpasst es insgesamt, die Mindestanforderungen in einer Form zu konkretisieren, welche die heutigen Begrifflichkeiten und Anforderungen der Datensicherheit aufnehmen. Der bürokratische Aufwand, welcher mit der Umsetzung der vorliegenden Verordnung verbunden ist, entspricht nicht dem Verhältnismässigkeitsprinzip. Für die Verantwortlichen ergibt sich ein unübersichtlicher Detaillierungsgrad, der in keiner Weise Rücksicht auf die Realität der Spitäler nimmt.

[1] Mehr Informationen: 20200630_Positionierung_Qualitaetsentwicklung_Gesetzlicher_Rahmen_V1.0_D.pdf (hplus.ch)

H+ setzt sich ein für geeignete rechtliche Rahmenbedingungen, um qualitativ hohe medizinische Behandlungen und ein effizientes Spitalwesen zu fördern. Dabei spielen datenschutzrechtliche Aspekte unbestritten eine wichtige Rolle. **Im vorliegenden Fall gehen die datenschutzrechtlichen Vorschriften aber über das hinaus, was gewollt und geboten ist und stellen damit eine unnötige administrative Hürde dar, die den Spitalalltag massiv beeinflussen. Einmal mehr werden fundamentale demokratie-politische Grundsätze untergraben. H+ lehnt die vorliegende Vernehmlassungsvorlage deshalb ab.** Dies gilt insb. für die folgenden Regelungen, die keine Detailvorschriften sind, sondern in ihrer Bedeutung viel eher den im nDSG enthaltenen Bestimmungen gleichkommen:

- Bearbeitungsreglement privater Personen (Art. 4 E-VDSG)
- Information bei der Bekanntgabe von Personendaten (Art. 15 und 16 E-VDSG)
- Dokumentationspflichten (bspw. Art. 19 Abs. 5 und Art. 20 Abs. 5 E-VDSG)

2. Datensicherheit

2.1. Allgemeiner Teil

Mit den Bestimmungen zur Datensicherheit erfüllt der Bundesrat den gesetzlichen Auftrag, die Mindestanforderungen an die Datensicherheit auf Verordnungsstufe zu präzisieren (Art. 8 Abs. 3 nDSG). An diese Mindestanforderungen knüpft zudem die Strafnorm in Artikel 61 Buchstabe c nDSG an. Der Grad an Sicherheit, der eingehalten werden muss, damit die Strafnorm nicht verletzt wird, bestimmt sich dabei nach den Grundsätzen und Kriterien des vorliegenden, ersten Abschnittes. Im E-VDSG wurde auf ein starres Regime von Mindestanforderungen verzichtet, da sich keine allgemeingültigen Mindestanforderungen für jegliche Branchen festlegen lassen. Der Ansatz des E-VDSG beruht – entsprechend dem Gesetz – auf einem risikobasierten Ansatz: Je höher die Gefährdung für die Persönlichkeitsrechte und die Grundrechte des Einzelnen, desto höher die Anforderungen.

H+ lehnt die Bestimmungen in diesem Abschnitt ab, sofern ihnen eine gesetzliche Grundlage fehlt bzw. sie dem Willen des Gesetzgebers widersprechen. Die Bestimmungen sind zu detailliert und tragen damit der Vielfalt der Bearbeitungsaktivitäten und Situationen keine Rechnung. Regelungen nach dem Giesskannenprinzip bringen keine Rechtssicherheit, sondern bewirken eher das Gegenteil. Für H+ ist es unverständlich, dass verbreitet angenommen wird, dass mit engmaschiger Kontrolle und damit massiv mehr administrativem Aufwand automatisch eine bessere Durchsetzung des Datenschutzes erfolgt. Ganz im Sinne von «vor lauter Bäumen den Wald nicht mehr sehen» ist H+ der Auffassung, dass die vorliegenden Regelungen, am Ziel und Zweck für mehr Datensicherheit vorbeischiessen und die aktuell noch nicht abschätzbaren, negativen Folgen überwiegen.

2.2. Besonderer Teil

Art. 3 Abs. 1: Protokollierung

Kommentar: Unternehmen müssen gemäss dem Wortlaut von Art. 3 Abs. 1 E-VDSG Datenbearbeitungen protokollieren, wenn sich aus der Datenschutz-Folgenabschätzung ergibt, dass trotz der ergriffenen Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht. Gemäss dem erläuternden Bericht besteht der Zweck der Protokollierung darin, dass Bearbeitungen von Personendaten nachträglich überprüfbar sind, so dass im Nachhinein festgestellt werden kann, ob Daten abhandengekommen sind oder gelöscht, vernichtet, verändert oder offengelegt wurden. Ausserdem geht es auch um die Gewährleistung der Zweckkonformität. So können sich aus der Protokollierung auch Hinweise ergeben, ob Personendaten zweckkonform bearbeitet wurden. Weiter können die Protokollierungen auch dazu dienen, Verletzungen der Datensicherheit aufzudecken und aufzuklären. Die Protokollierung hat hingegen nicht zum Ziel, die Nutzerinnen und Nutzer, die Personendaten bearbeiten, zu überwachen.
Diese Bestimmung ist aus Sicht der Spitäler in mehrfacher Hinsicht bedenklich:

- Sollte diese Bestimmung so umgesetzt werden, bedarf es eines riesigen Überwachungsapparats, welcher viele Ressourcen (finanziell wie auch personell) binden würde.
- Die Norm dient nicht primär der Protokollierung zur Gewährleistung der Datensicherheit, sondern vielmehr der nachträglichen Feststellung, ob es zu einer unbefugten Datenbearbeitung gekommen ist. Die Norm widerspricht damit dem Gesetz, weil sie sich zur Feststellung einer Verletzung der Datensicherheit[2] nicht eignet und damit unverhältnismässig ist.

[2] Art. 8 revDSG, welcher als Grundlage der Bestimmung dient, behandelt nur die Datensicherheit i.e.S. Nur solche sollte der Bundesrat gemäss Art. 8 Abs. 3 revDSG ausführen und nur die Verletzung solcher können auch zu einer Strafbarkeit führen.

- Das Ergebnis einer Datenschutz-Folgenabschätzung (DSFA) wird in der Regel nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenbearbeitung. Das hat mit der Datensicherheit nichts zu tun. Folglich ist das Ergebnis der DSFA kein geeigneter Indikator, um das Risiko einer Verletzung der Datensicherheit festzustellen.

Punktuelle Pflichten zur Protokollierung mögen durchaus sinnvoll sein (bspw. zur Auswertung von Logs zu Analysezwecken); eine solche pauschale Norm lehnt H+ indessen klar ab, da sie schlicht unverhältnismässig ist. Die Erläuterungen des E-VDSG (so auch Art. 3 Abs. 3) bestätigen sogar, dass es (auch) um die Gewährleistung der zweckkonformen Bearbeitung geht. Das widerspricht klar dem Gesetzgebungsauftrag.

Art. 4: Bearbeitungsreglement von privaten Personen

Kommentar: Art. 4 E-VDSG enthält die Pflicht zur Erstellung eines Bearbeitungsreglements. Entsprechend dem risikobasierten Ansatz der Vorgabe der Datensicherheit soll ein Bearbeitungsreglement immer dann erstellt werden, wenn ein erhöhtes Risiko vorliegt. So müssen private Verantwortliche ein Bearbeitungsreglement für automatisierte Bearbeitungen erstellen, u.a. wenn sie umfangreich besonders schützenswerte Personendaten bearbeiten (Bst. a).
Systematisch wird dies bei der Datensicherheit geregelt, aber ein Bearbeitungsreglement ist offenkundig keine Datensicherheitsmassnahme, sondern dient der Einhaltung der Datenbearbeitungsgrundsätze und damit dem Datenschutz. Auch bei der vorliegenden Bestimmung fehlt dementsprechend die gesetzliche Grundlage (s. oben). Dabei steht der beträchtliche Aufwand für die Bewirtschaftung eines solchen Bearbeitungsreglements in keinem Verhältnis (massive Ausdehnung der Dokumentationspflichten, die weit über das Gebotene herausgehen).
Überdies gilt es folgende Punkte zu kritisieren:

- Die wesentlichen Angaben werden ohnehin bereits im Rahmen der in solchen Fällen erforderlichen Datenschutz-Folgenabschätzung dokumentiert, der Rest im ohnehin zu erstellenden Inventar.
- Auch die DSGVO sieht eine solche Regelung nicht vor (sog. «Swiss Finish»).
- Zweifellos können besonders heikle Datenbearbeitungen eine betriebsinterne Regelung erfordern. Dieser Aspekt ist jedoch über Art. 7 Abs. 1 revDSG bereits hinreichend geregelt.

Die Bestimmung ist damit unnötig restriktiv und aus Sicht von H+ zu streichen.

3. Pflichten des Verantwortlichen und des Auftragsbearbeiters

3.1. Allgemeiner Teil

Im 2. Kapitel werden die Informations- und Meldepflichten konkretisiert. Art. 13 Abs. 1 E-VDSG impliziert eine Informationspflicht des Auftragsbearbeiters, was auch aus dem erläuternden Bericht (S. 30) explizit hervorgeht. Das revDSG sieht aber keine Informationspflicht des Auftragsbearbeiters vor; gemäss Art. 19 revDSG besteht diese – richtigerweise – nur für den Verantwortlichen. Da das Gesetz keine solche Pflicht für den Auftragsbearbeiter vorsieht, kann sie auch nicht über die Verordnung eingeführt werden. Das gilt für alle Artikel im zweiten Kapitel gleichermassen, sofern sie Informationspflichten betreffen.

3.2. Besonderer Teil

Art. 15 und 16: Information bei der Bekanntgabe sowie über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten

Kommentar: Nebst der «Aktualität» und der «Zuverlässigkeit» der Personendaten wird im Rahmen der Informationspflicht bei der Bekanntgabe von Personendaten in *Artikel 15* neu die «Vollständigkeit» erwähnt. Mit anderen Worten dürfen die Daten, welche herausgegeben werden, nicht lückenhaft sein. Bei dieser Vorschrift beisst sich die Katze in den Schwanz: Der Empfänger ist selbst verpflichtet, die Bearbeitungsgrundsätze einzuhalten und angemessene Massnahmen zu treffen, sich über die Richtigkeit der Daten zu vergewissern. Eine entsprechende Information durch die übermittelnde Person unterläuft dies bzw. macht eine der möglichen Vergewisserungsmassnahmen zum allein gültigen Massstab. Dies widerspricht dem Gesetz. Die Regelung ist überdies in der Praxis nicht umsetzbar; sind Daten lückenhaft, dürfte der Auftragsbearbeiter sie also gar nicht herausgeben bzw. er soll etwas bekanntgeben, das er gar nicht hat.

Die Pflicht des Datenverantwortlichen, die Empfänger über sämtliche Veränderungen in den Personendaten (Berichtigung, Löschung oder Vernichtung der Bearbeitung) zu informieren, wie sie in *Artikel 16* E-VDSG vorgesehen ist, widerspricht dem Willen des Gesetzgebers: Die Bestimmung war bereits im Entwurf des revDSG vorgesehen und wurde vom Parlament gestrichen. Sie kann daher nicht über die revidierte Verordnung eingeführt werden.
Sollte die Bestimmung wie vorgesehen umzusetzen sein, würde dies, gerade für die Spitäler, einen enormen, gar unüberblickbaren, Aufwand bedeuten.

Die beiden Normen sind aus Sicht von H+ zu streichen, weil sie einen enormen Aufwand bedeuten würden und praktisch nicht umsetzbar sind.

Art. 19 Abs. 5

Kommentar: Bereits die Botschaft zum revDSG hielt fest, dass keine allgemeine Dokumentationspflicht eingeführt werden soll (S. 6978). Diese soll nun aber mittels dem vorliegenden Verordnungsentwurf durch die Hintertür verankert werden. Das würde aber die allgemeingültigen gesetzgeberischen Regeln unterlaufen.
Des Weiteren bleibt freilich unklar, was der Nutzen der Dokumentations- und Auskunftspflicht sein soll, wenn sich aus der Systematik klar ergibt, dass nur meldepflichtige Verletzungen zu dokumentieren sind. Wird eine Verletzung gemeldet und ist diese für den EDÖB von Interesse, wird er den Sachverhalt untersuchen, aber kaum später darauf zurückkommen. Der Nutzen wäre also auch für den EDÖB keinen.

Dasselbe gilt im Übrigen auch für Art. 20 Abs. 5 bei der Pflicht zur Dokumentation der Verweigerungs-, Einschränkungs- und Aufschubsgründen im Falle eines Auskunftsbegehrens. *Diese Norm ist im Übrigen auch wenig zweckmässig. Die betroffene Person erhält eine Antwort auf ihr Ersuchen. Will sie dagegen vorgehen, kann sie diese Antwort ins Recht legen. Die Bestimmung sorgt nur für zusätzlichen Aufwand (längere Aufbewahrungszeit bzw. höhere Kadenz der Datenbeantwortung als notwendig).*

Die beiden Bestimmungen bringen keinen Mehrwert, sind operativ ausgesprochen aufwendig und haben keine gesetzlichen Grundlagen. Sie sind deshalb zu streichen.

4. Weiteres

Im Übrigen schliessen wir uns der allgemeinen Stellungnahme des Vereins für Unternehmens-Datenschutz (VUD) an.

* * * * *

Wir danken Ihnen für die Aufnahme unserer Anliegen und stehen Ihnen für ergänzende Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Anne Bütikofer
Direktorin

HANDELSVERBAND
ASSOCIATION DE COMMERCE
.SWISS

per email:
jonas.amstutz@bj.admin.ch

Frau Bundesrätin
Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz Stellung beziehen zu dürfen. Wir nehmen in unserer Stellungnahme das Kapitel 5 Bundesorgane explizit aus und überlassen die inhaltliche Beurteilung den betroffenen Behörden.

Generell stellen wir fest, dass die Verordnung zum Bundesgesetz über den Datenschutz unbefriedigend ist. Erstens wird versucht auf dem Verordnungsweg im Gesetzgebungsprozess eliminierte Regeln über die "Hintertür" wieder einzuführen. Zweitens finden wir Swiss Finish Komponenten, welche einer angestrebten Harmonisierung mit der DSGVO widerlaufen. Drittens werden nicht erfüllbare Forderungen aufgestellt bzw. Terminologien verwendet, welche in Theorie gut tönen, in Realität aber schlicht nicht umsetzbar sind. Die Verordnung bedarf einer grundlegenden Überarbeitung und Korrektur.

HANDELSVERBAND.SWISS
CH-3000 Bern
Tel. + 41 58 310 07 17
info@handelsverband.swiss
www.handelsverband.swiss

HANDELSVERBAND.swiss als Vertreter des digitalen Handels in der Schweiz

Unser Verband vertritt 380 Unternehmen (juristische Personen), welche über 400 Webshops aber auch stationären Handel betreiben. Die angeschlossenen Unternehmen sind verantwortlich für rund 70 % des B2C-Onlinehandels in der Schweiz und übergaben 2020 rund 85 Mio Pakete (inkl. Retouren) an die Schweizerische Post. In anderen Worten: Unsere Mitglieder generieren mittlerweile rund 45 % des Paketvolumens der Schweizerischen Post und sind insbesondere über die Aktivitäten im Onlinehandel sehr direkt von der Revision des Datenschutzes betroffen. Daneben betreiben unsere Mitglieder stationäre Verkaufseinheiten, häufig gekoppelt mit Kundenkarten und/oder Loyalitätsprogrammen oder anderen Datenerfassungen im Kontext von Kundendaten. Alle Mitglieder zusammen generieren rund 20 Mrd. Umsatz mit Privatkonsumenten (B2C) aber auch im Handel mit Unternehmen (B2B).

Jedes unserer Mitglieder ist entsprechend direkt vom neuen DSG (nDSG) und der entsprechenden Verordnung (nachstehend E-VDSG) betroffen. Insbesondere arbeitet der Onlinehandel mit vielen Drittdienstleistern (Postleistungen, Bonität, Shopsysteme, Payment etc.), die Auftragsdatenverarbeitung mit entsprechender Weitergabe und Speicherung von Kundendaten ist Teil des Geschäftsmodells, um Verträge überhaupt erfüllen zu können.

Unser Verband hat bereits im Jahre 2018 Mittel eingesetzt und Wege beschritten, seine Mitglieder zu einer Befolgung der EU-DSGVO zu motivieren – zu verflochten sind heute Datenströme in Europa aber auch in andere Länder (insbesondere USA). Der Einsatz von Dritt-Software und Clouddiensten ist "Tagesgeschäft" und das Zusammenspiel mit international agierenden Zahlungsanbietern Normalität. In diesem Kontext ist es unabdingbar, dass auch die VDSG sich an internationalen Gegebenheiten orientiert und keine teure und illusorische Sonderregeln im Sinne eines Swiss Finish vorschreibt. Ein besonderes Augenmerk gilt auch den KMU Händlern, welche alleingestellt mit dem Regelwerk in vielerlei Hinsicht überfordert sein dürften. Unser Verband erachtet es als zentrale Aufgabe, das nun vorliegende Gesetzes- und Verordnungs-Regelwerk auf umsetzbare Standards herunterzubrechen, um sowohl Privatkonsumenten als eben auch den Unternehmen grösstmöglichen Datenschutz gewährleisten zu können. In diesem Sinne erwarten wir eine Verordnung ohne Interpretationsspielraum, ohne "nachträgliche Gesetzgebung", ohne Wunschdenken und ohne Schweizer Sonderregelungen.

Artikel mit Swiss Finish

Folgende Verordnungsartikel beinhalten Swiss Finish Komponenten und sind diesbezüglich zu bereinigen bzw. zu streichen:

1. Art. 4 Abs. 1 E-VDSG
2. Art. 13 Abs. 1 E-VDSG
3. Art. 19 Abs. 5 E-VDSG

HANDELSVERBAND.swiss
CH-3000 Bern
Tel. + 41 58 310 07 17
info@handelsverband.swiss
www.handelsverband.swiss

Neue "gesetzgebende" Artikel

In folgenden Artikeln finden sich Regeln, welche entweder im Gesetzgebungsprozess bewusst eliminiert wurden, zum Gesetz widersprüchlich sind oder in der Verordnung als "neu gesetzgebend" erscheinen.

1. **STREICHEN** Artikel 3 E-VDSG: Protokollierungspflicht
2. **STREICHEN** Art. 13 E-VDSG: Widerspruch zu Art. 19 nDSG
3. **STREICHEN** Art. 16 E-VDSG: neue Informationspflicht
4. **STREICHEN** Art. 19 Abs. 1 Bst. b bis d: Neue Kriterien in Ergänzung zu nDSG Art. 24
5. **STREICHEN** Art. 19 Abs. 3: gesetzgebende Ergänzung zu Art. 24 Abs. 4 DSG
6. **STREICHEN** Art. 20 Abs. 5: gesetzgebende Ergänzung zu Art. 24

Definitionsfragen

- Was sind "automatisierte Systeme" im Sinne von Verordnung und Gesetz? Wir haben den Eindruck, dass damit nicht Systeme, sondern automatisierte Bearbeitungen und / oder selbstlernende Systeme gemeint sind. Der Begriff wird sowohl im Verordnungsentwurf (Art. 2 Bst. e und g) als auch im Bericht verwendet und ist zu klären.

- Schriftlichkeit / Dokumentieren: Aus unserer Sicht ist nicht klar geregelt, wie weit Schriftlichkeit bzw. Dokumentation in elektronischer Form gehen soll. Es wäre hilfreich, diese Begriffe klar zu definieren und unter Umständen zu separieren. Insbesondere betrifft die Fragestellung die "digitale Schriftlichkeit": Umfasst / beinhaltet dies auch elektronische Signaturen?

Zu den einzelnen Bestimmungen

Art. 1 Abs. 1 Bst. b

Per Definition wird eine Wahrscheinlichkeit mathematisch berechnet. Eine Eintretenswahrscheinlichkeit einer Datenverletzung zu berechnen dürfte für ein Unternehmen nicht möglich sein und sobald eine Verletzung eintritt ist die Wahrscheinlichkeit gleich eins. Es hilft dem Unternehmen also nicht, wenn es die Eintretenswahrscheinlichkeit als tief, mittel oder hoch einstuft und sich dann trotzdem ein "Unglück" ereignet. Wir empfehlen die "Eintretenswahrscheinlichkeit" als Kriterium zu eliminieren und durch "Folgen". Ansonsten müsste die Verordnung Kriterien zur Wahrscheinlichkeitsberechnung nennen.

Art. 1 Abs. 1 Bst. d

«Implementierungskosten» als Begriff in diesem Kontext als Kriterium zu verwenden ist nicht angebracht. Interne Aufwände, nicht verrechnete Aufwände von Partnern etc. werden in diesem Kontext nicht als Kosten verstanden. Wenn überhaupt wäre von Implementierungsaufwand zu sprechen, wobei auch dieser "relativ" zu verstehen wäre. Für ein kleines Unternehmen kann ein Implementierungsaufwand sehr gross sein, während es für das Grossunternehmen mit der gleichen Fragestellung einen kleinen Aufwand darstellt.

HANDELSVERBAND.swiss
CH-3000 Bern
Tel. + 41 58 310 07 17
info@handelsverband.swiss
www.handelsverband.swiss

Befremdet nehmen wir zudem zur Kenntnis, dass der Bericht auf Seite 16 die Implementierungskosten als nicht relevant darstellt:

"*Verantwortliche und Auftragsbearbeiter können sich insbesondere nicht mit der Begründung von der Pflicht einer angemessenen Datensicherheit befreien, dass damit übermässige Kosten verbunden sind; vielmehr müssen sie jedenfalls in der Lage sein, eine angemessene Datensicherheit zu gewährleisten."*

Gemäss dieser Aussage ist es also nicht relevant, wie hoch die Kosten sind, die Datensicherheit muss unabhängig davon angemessen sein. Wenn dies die Ansicht des Bundesrates ist, könnte man die "Implementierungskosten" als Kriterium auch streichen.

Art. 1 Abs. 2

Diese Bestimmung ist nicht korrekt formuliert. Die getroffenen Massnahmen sind nur dann zu überprüfen, wenn sich Rahmenbedingungen gemäss Art. 1 Abs 1 Bst a – c ändern. Zudem stellt sich die Frage, ob sich mit veränderndem Implementierungsaufwand gemäss Art. 1 Abs 1 Bst. d die organisatorischen Massnahmen verändern sollten (siehe auch vorhergehende Bemerkung)

Art. 2, Einleitungssatz

Die Schutzziele müssen als Ableitung von Artikel 1 formuliert werden: "Soweit gemäss Artikel 1 angemessen, müssen... "

Art. 2, Bst. g:

Was ist ein "automatisiertes System"? Müsste nicht eher von automatisierten Prozessen gesprochen werden? Zudem steht die Eingabekontrolle im Widerspruch zum vom Parlament entschiedenen Verzicht auf die Protokollierungspflicht (siehe auch Artikel 3).

Art. 2, Bst. j:

Die formulierte Schutzziel ist fern jeder Realität. Wie soll ein Unternehmen gewährleisten, dass Cloud Dienste jederzeit verfügbar sind? Wie kann vom Verantwortlichen sichergestellt werden, dass Dritt-Software automatisch Fehler melden? Dieser Buchstabe ist überflüssig und zu streichen.

Art. 3

Das Parlament hat im Gesetzgebungsprozess bewusst auf eine Protokollierung verzichtet. Insofern ist die nachgelagerte Einführung einer Protokollpflicht nicht angebracht. Dieser Artikel ist zu streichen.

Die Ausführung im Erläuterungsbericht zum Inhalt des vorgeschlagenen Artikels ist zudem widersprüchlich: Einerseits spricht er von "Protokollierung bei automatisierter Bearbeitung" (siehe auch Definitionsfragen), andererseits geht er davon aus, dass die bearbeitenden Mitarbeiter mitgespeichert werden. Entweder betrifft die Protokollierung die automatisierte Bearbeitung oder die manuelle Bearbeitung. Falls nur die automatisierte Bearbeitung protokolliert werden sollte, können auch keine Daten zur Identität der bearbeitenden Person gespeichert werden.

Die im Absatz 4 geforderte systemische Trennung von Datenbearbeitung und Protokollierung ist realitätsfremd – insbesondere die Begründung mit Cyberangriffen ist abenteuerlich. Ein Cyberangriff dürfte weniger Interesse daran haben Protokolle zu verändern als vielmehr Daten generell zu

entwenden, manipulieren oder zu löschen. Getrennt aufbewahrte Protokolle helfen dabei nicht den Schaden zu verhindern.

Art. 4

Absatz 3 beginnt mit den Worten "Die private Person muss... ". Was möchte uns der Gesetzgeber mit dieser Formulierung sagen? Müsse dies nicht "Der/die Verantwortliche und Auftragsverarbeiter müssen... " heissen?

Art. 6, Abs. 1 und 2

Die geforderte Pflicht für den Verantwortlichen, die vertrags- und gesetzesmässige Bearbeitung durch den Auftragsbearbeiter "sicherzustellen" ist nicht realisierbar. Mit Übergabe an einen Auftragsbearbeiter verliert der Daten-Verantwortliche an Einfluss und hat kaum mehr die Möglichkeit den Datenschutz beim Dritten selbst "sicherzustellen". Er kann wohl Prüfungen vornehmen und sich "vergewissern" oder aber sich den Datenschutz durch den Bearbeiter vertraglich bestätigen lassen. Hingegen kann er nicht selbst als Verantwortlicher "sicherstellen". Dies müsste im Artikel entsprechend korrigiert werden.

Art. 8 Abs 1 bis 3

Es ist einem Verantwortlichen nicht zumutbar, diese Beurteilung eigenständig vorzunehmen. Gemäss erläuterndem Bericht wird auch klargestellt, dass sich diese Bestimmung an den Bundesrat richten soll. Entsprechend wäre dies im Verordnungstext explizit festzuhalten.

Art. 9 Abs. 2

Auch hier ist die Forderung an den Verantwortlichen überrissen, wenn er «sicherstellen» muss. Es reicht "angemessene Massnahmen zu treffen, dass ...."

Art. 10 Abs. 1

Auch hier ist die Forderung an den Verantwortlichen überrissen, wenn er «sicherstellen» muss. Es reicht "angemessene Massnahmen zu treffen, dass ...."

Art. 13 Abs. 1

Gemäss Art. 19 Abs. 1 nDSG liegt die Informationspflicht beim Verantwortlichen und nicht beim Auftragsbearbeiter. Es kann zwar allenfalls eine vertragliche Delegation der Pflichterfüllung stattfinden, aber grundsätzlich ist es systemwidrig beide gleichzeitig in die Pflicht zu nehmen.

Art. 16

Diese Bestimmungen wurde im Zuge der parlamentarischen Diskussion auf Gesetzesstufe abgelehnt. Es ist nicht angebracht, diese Bestimmung nun auf dem Verordnungsweg wieder einzuführen.

Art. 17

Dieser Artikel ist zu streichen. Der Zusatz "... so darf sie deswegen nicht benachteiligt werden" ist nicht realistisch umzusetzen. Die betroffene Person fühlt sich mit dem Hinterfragen der automatisierten Einzelentscheidung in den meisten Fällen per se benachteiligt (z.B., wenn kein Kauf auf Rechnung angeboten wird) und es ist einem Anbieter erlaubt seine Vertragspartner auszusuchen. Sollten automatisieren Einzelentscheidungen aufgrund fehlerhafter Personendaten zustande kommen, steht den Betroffenen das Recht auf Auskunft/Berichtigung uneingeschränkt zur Verfügung (siehe Art 20 ff E-VDSG).

Art. 18

Es stellt sich die Frage nach der "Schriftlichkeit" in elektronischer Form: Ist mit der elektronischen Form ein Dokument ohne digitale Signatur gültig oder nicht? Es ist davon auszugehen, dass die Digitalisierung laufend neue Datenbearbeitungen mit sich bringt und dafür standardisierte, digitale Prozesse aufgebaut werden. Sind solche digital dokumentierten Prozesse ohne Signaturen ausreichend? Falls nein, wäre der Wortlaut entsprechend anzupassen. Überhaupt ist das Thema "Schriftlichkeit" im Kontext von Datenbearbeitung abschliessend und eindeutig zu definiere (siehe Definitionsfragen)

Art 19 generell

Dieser Verordnungsartikel rezitiert den vorhandenen umfassenden Gesetzesartikel und fügt neue gesetzgeberische Vorschriften hinzu, welche gemäss nDSG Artikel 24 nicht vorgesehen sind.

Art. 19 Abs. 1 Bst. b bis d

Diese Kriterien sind dem Gesetz nicht zu entnehmen. Es ist ferner nicht definiert was mit "Kategorien" im Zusammenhang mit Personen gemeint ist. Der Bundesrat hat weder eine Delegation noch eine Ermächtigung erhalten, Art. 24 nDSG zu ergänzen. Deshalb sind diese Buchstaben aus der Verordnung zu streichen.

Ar. 19 Abs. 1 Bst. e

Bei der Entdeckung einer Verletzung der Datensicherheit ist es meistens nicht möglich, die Folgen und die allfälligen Risiken umgehend und abschliessend festzustellen. Hier wäre ein vorangehendes "soweit möglich" oder "Mögliche Folgen" ebenfalls angebracht

Art. 19 Abs. 3

Siehe Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das nDSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er über Art. 24 Abs. 4 nDSG hinausgeht.

Art. 19 Abs. 5

Siehe Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das nDSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 nDSG hinausgeht, der keine Dokumentationspflicht enthält.

HANDELSVERBAND.SWISS
CH-3000 Bern
Tel. + 41 58 310 07 17
info@handelsverband.swiss
www.handelsverband.swiss

Art. 23

Grundsätzlich gilt gemäss nDSG, dass eine Auskunft kostenlos sein muss. Es stellt sich mit dem E-VDSG die Frage was ein "unverhältnismässiger Aufwand" für eine Auskunftserteilung darstellt. Weiter scheint die in Abs. 2 limitierte Kostenbeteiligung von 300 CHF sehr tief zu sein, wenn ein Aufwand unverhältnismässig ist. Hier hätten wir uns mehr und genauere Vorgaben in der Verordnung erhofft.

Weiter fehlt eine Einschränkung bzw. Spezifizierung zu nDSG Art. 26 Abs 1 c, wie missbräuchliche Massen-Anfragestellungen beantwortet werden sollen oder dass diese ausserordentliche Kostenbeteiligungen nach sich ziehen können.

Art. 26

Der Klärungsversuch für Ausnahmeregelungen zur Führung eines Verzeichnisses von Bearbeitungstätigkeiten gemäss Bst. a und b lässt weiterhin Fragen offen. Insbesondere das Wort "umfangreich" ist schwierig einzuordnen. Hier wünschen wir uns konkretere Vorgaben um klare Grenzen ziehen und Instruktionen geben zu können. In welcher Hinsicht ist das Wort umfangreich zu definieren? Geht es um die Anzahl Personendaten, die Anzahl Bearbeitungen/Transaktionen pro Jahr oder welche Kriterien sollen hier zugrunde gelegt werden?

Art. 45 Abs. 1 und 2

Wir verweisen auf unsere Bemerkungen zu Artikel 23 E-VDSG, vor allem im Zusammenhang mit missbräuchlichen Anfragen. Es wäre begrüssenswert, wenn auch betroffene Firmen Stundenansätze wie in Artikel 2 definiert abrechnen könnten.

Wir danken Ihnen für die Berücksichtigung unserer Argumente und stehen für Auskünfte jederzeit gerne zur Verfügung.

Freundliche Grüsse

HANDELSVERBAND.swiss

Tomas Prenosil Patrick Kessler

HANDELSVERBAND.swiss
CH-3000 Bern
Tel. + 41 58 310 07 17
info@handelsverband.swiss
www.handelsverband.swiss

HÄRTING

HÄRTING Rechtsanwälte AG

Landis + Gyr-Strasse 1
6300 Zug
+41 41 710 28 50
office@haerting.ch
www.haerting.ch

Eidgenössisches Justiz und
Polizeidepartement EJPD
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

BETREFF

Vernehmlassung VDSG
Stellungnahme zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

DATUM

14. Oktober 2021

ANSPRECHPERSON	E-Mail	TELEFON
RA lic. iur. Nicole Beranek Zanon	beranek@haerting.ch	+41 41 710 28 50

Sehr geehrte Frau Bundesrätin Keller-Sutter,
Sehr geehrter Herr Amstutz,
Sehr geehrte Damen und Herren,

Wir bedanken uns für die Möglichkeit zum rubrizierten Geschäft Stellung zu beziehen und nehmen diese gerne fristgerecht wie folgt wahr:

Art. 1 Grundsätze

[1] Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:

a. Zweck, Art, Umfang und Umstände der Datenbearbeitung;
b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen;
c. der Stand der Technik;
d. Implementierungskosten.

[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.

Neuer Vorschlag

[…]

b. die verbleibende Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen, nach Implementierung der Massnahmen;
c. die allgemein anerkannten Regeln der Technik;

[…]

Begründung

Der erläuternde Bericht weist darauf hin, dass nicht jede Verletzung der Datensicherheit i.S.v. Art. 5 lit. h nDSG auch eine Verletzung der Mindestanforderungen i.S.v. Art. 8 Abs. 3 nDSG und somit eine Verletzung der Sorgfaltspflichten gemäss Art. 61 lit. c nDSG darstellt, denn eine absolute Sicherheit könne nicht verlangt werden. Im diesem Sinne ist bei der Beurteilung, ob die technische oder organisatorische Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessen sind, unter anderem das Restrisiko einer Verletzung der Datensicherheit zu prüfen. Entsprechend ist zu präzisieren, dass es sich um die Eintretenswahrscheinlichkeit nach den ergriffenen Mitigationsmassnahmen handelt.

Ebenso sollte man den Stand der Technik präzisieren. Stand der Technik ist eine Technikklausel, die in verschiedenen Rechtsgebieten Verwendung findet. Man versteht darunter den bekannten technischen Entwicklungsstand und die darauf basierenden technischen Möglichkeiten zur Erreichung eines bestimmten praktischen Ziels. Es handelt sich deshalb um mehr als nur die allgemein anerkannten Regeln der Technik. Dies würde aber erfordern, dass jeder einen Kenntnisstand weit über den anerkannten Regeln der Technik hat und diese anwendet. Gerade im Lichte dessen, dass die Verletzung der Datensicherheit neu Straffolgen nach sich zieht, sollte man diesen Massstab auf das reduzieren, was der Rechtsanwender bis anhin unter dieser Formulierung verstanden hat, nämlich die Anwendung der anerkannten Regeln der Technik.

Art. 2 Schutzziele

Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen:

a. Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen.
b. Zugangskontrolle: Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt.
c. Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht.
d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert.
e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert.

f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.
g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden.
h. Bekanntgabekontrolle: Es kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden.
i. Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden.
j. Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).
k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.

Neuer Vorschlag

Soweit angemessen und geeignet, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele anstreben:

[…]

l. Rechenschaftspflicht: Es wird gewährleistet, dass berechtigte Personen, welche die Datensicherheitziele missachten, zur Rechenschaft gezogen werden.
m. Verbesserungskontrolle: es sind kontinuierliche Verbesserungsprozesse zu implementieren, indem Risiken ermittelt, reduziert und kontinuierlich behandelt werden.

Begründung

Gemäss erläuternder Bericht enthält Art. 2 eine Auflistung der Schutzziele, auf welche die Massnahmen auszurichten sind. Dabei sei vorstellbar, dass nicht jedes Schutzziel in jedem Fall von Relevanz sei. Da auch hier wieder daran zu erinnern sei, dass eine absolute Datensicherheit nicht verlangt werden kann, ist Art. 2 anzupassen, indem die Geeignetheit eines anstrebenswerten Schutzzieles mitzuberücksichtigen ist.

In einer neuen Ziffer l) ist zu ergänzen, dass berechtigte Personen, die sich nicht an die Sicherheitsziele halten, firmenintern zur Rechenschaft zu ziehen sind. Nebst der Rechenschaftspflicht soll auch mit einer neuen Ziffer m) eine kontinuierliche Verbesserung Ziel der Datensicherheit sein, da die Technik sich ständig weiterentwickelt.

Art. 3 Protokollierung

[1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.

[2] Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.

Neuer Vorschlag

[1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter soweit technisch möglich zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.

Begründung

Grundsätzlich ist die Protokollierung zu begrüssen, allerdings ist sie nicht immer und überall technisch möglich, weshalb u.E. eine Ergänzung notwendig ist.

Art. 4 Bearbeitungsreglement von privaten Personen

[1] Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie:

a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder
b. ein Profiling mit hohem Risiko durchführen.

[2] Das Reglement muss mindestens Angaben enthalten:

a. zum Bearbeitungszweck;
b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
d. zur internen Organisation;
e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung;
f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit;
g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe;
h. zu den Massnahmen, die zur Datenminimierung getroffen werden;
i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung;

j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.

[3] Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.

Neuer Vorschlag

Art. 4 streichen.

Begründung

Das Bearbeitungsreglement entbehrt einer gesetzlichen Grundlage im nDSG. Die Heranziehung von Art. 8 Abs. 3 nDSG *("*Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit") genügt hierbei nicht. Art. 4 nVDSG geht auch über die Anforderungen der DSGVO hinaus und schafft damit einen unnötigen Schweizer Mehraufwand.

Art. 5 Bearbeitungsreglement von Bundesorganen

[1] Das verantwortliche Bundesorgan und dessen Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie:

a. besonders schützenswerte Personendaten bearbeiten;
b. ein Profiling durchführen;
c. Datenbearbeitungen im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG ausführen;
d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen werden Personendaten zugänglich machen;
e. Datenbestände miteinander verknüpfen; oder
f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.

[2] Das Reglement muss mindestens die Angaben nach Artikel 4 Absatz 2 enthalten.

[3] Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen.

Neuer Vorschlag

Art. 5 streichen.

Begründung

Siehe Begründung für Art. 4.

Art. 6 Modalitäten

[1] Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.

[2] Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.

[3] Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich genehmigt hat.

Neuer Vorschlag

[1] Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss in angemessener Weise sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.

Abs. 2 streichen.

Begründung

Betr. Abs. 1: Der Verantwortliche hat nicht in jedem Fall sicherzustellen, dass die die Daten vertrags- oder gesetzesgemäss bearbeitet werden, sondern muss in angemessener Weise dafür Sorge tragen.

Abs. 2 stellt sinngemäss eine Wiederholung von Art. 16 ff. nDSG dar und enthält keine zusätzlichen Angaben.

Art. 8 Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs

[1] Werden Personendaten ins Ausland bekanntgegeben, so müssen bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden:

a. die internationalen Verpflichtungen des Staates oder internationalen Organs im Bereich des Datenschutzes;
b. die Achtung der Menschenrechte;
c. die geltende Gesetzgebung zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung;
d. die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes;
e. das wirksame Funktionieren von einer oder mehreren unabhängigen Behörden, die im betreffenden Staat mit dem Datenschutz beauftragt sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen.

[2] Bei der Beurteilung können die Einschätzungen von internationalen Organen oder ausländischen Behörden, die für den Datenschutz zuständig sind, berücksichtigt werden.

[3] Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch neu beurteilt.

[4] Ergibt sich aus einer Beurteilung nach Absatz 3 oder aus verfügbaren Informationen, dass ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ kein angemessener Datenschutz mehr gewährleistet, so wird der Entscheid gemäss Artikel 16 Absatz 1 DSG geändert, sistiert oder aufgehoben. Dieser neue Entscheid hat keine Auswirkungen auf bereits erfolgte Datenbekanntgaben.

[5] Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz sind in Anhang 1 aufgeführt.

[6] Der EDÖB wird vor jedem Entscheid über die Angemessenheit des Datenschutzes konsultiert.

Neuer Vorschlag

[1] Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~ muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen ~~t werden~~:

[…]

Begründung

Da Art 8 sich alleine an den Bundesrat richtet, ist dies entsprechend klarzustellen. Es kann nicht Aufgabe der Wirtschaftsteilnehmer sein, diese Fragen für sich zu prüfen, da dies KMU's stark belasten würde.

Art. 9 Datenschutzklauseln und spezifische Garantien

[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen mindestens die folgenden Punkte regeln:

a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung und der Richtigkeit;
b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen;
c. die Art und der Zweck der Bekanntgabe von Personendaten;
d. die Namen der Staaten, in die Personendaten bekanntgegeben werden;
e. die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden;
f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;
g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger;
h. die Massnahmen zur Gewährleistung der Datensicherheit;
i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;

j. die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren;
k. die Rechte der betroffenen Person, namentlich:
    1. das Auskunftsrecht,
    2. das Widerspruchsrecht,
    3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten,
    4. das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen.

[2] Der Verantwortliche muss angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.

[3] Wurde der EDÖB über die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die:

a. unter denselben Datenschutzklauseln oder Garantien erfolgen, soweit die Kategorien der Empfängerinnen und Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder
b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen Unternehmen, die zum selben Konzern gehören, stattfinden, soweit die Datenschutzklauseln oder Garantien weiterhin einen geeigneten Datenschutz gewährleisten.

Neuer Vorschlag

g. die ~~zur Bearbeitung der Daten berechtigten~~ Empfängerinnen und Empfänger;

[…]

j. die Pflicht ~~der Empfängerin oder des Empfängers~~, die betroffenen Personen über die Bearbeitung im Sinne von lit. i zu informieren;

k. die Rechte der betroffenen Person, namentlich:
    1. das Auskunftsrecht,
    2. das Recht eine Einwilligung jederzeit zu widerrufen,

[…]

Begründung

Allgemeine Anmerkung zu Art. 9: Die Anforderungen in Art. 9 sollten sich an den Rollen von Exporteur und Importeur orientieren.

Betr. lit. j: Da es sich hierbei wohl um «onward transfer» handelt, sollte hierbei Bezug auf lit. i genommen werden. Zudem kann offengelassen werden, ob die Informationspflicht dem Exporteur oder Importeur aufgelegt werden soll.

Betr. lit. k: Das neue DSG kennt als Widerspruchsrecht nur das Recht der betroffenen Person Widerspruch gegen die Bekanntgabe von Personendaten durch das verantwortliche Bundesorgan einzulegen (Art. 37 nDSG). Dies dürfte hier in Art. 9 Abs. 1 lit. k wohl kaum gemeint sein. Der erläuternde Bericht bezeichnet hierbei «das Recht Widerspruch gegen die Bearbeitung von

Personendaten einzulegen». Es wird dabei nicht ersichtlich, auf welches Recht der betroffenen Personen in der nDSG Bezug genommen wird. Es dürfte sich hier um das Recht der betroffenen Person handeln, ihre erteilte Einwilligung jederzeit zu widerrufen, weswegen lit. k in diesem Sinne anzupassen ist.

Art. 10 Standarddatenschutzklauseln

[1] Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.

[2] Der EDÖB veröffentlicht eine Liste von Standarddatenschutzklauseln, die er genehmigt, ausgestellt oder anerkannt hat.

Neuer Vorschlag

[1] Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um dazu beizutragen ~~sicherzustellen~~, dass die Empfängerin oder der Empfänger diese beachtet.

Begründung

Betr. Abs. 1: Der Verantwortliche kann in der Regel nicht sicherstellen, dass der Empfänger die Standarddatenschutzklauseln beachtet, jedoch muss er hierzu beitragen.

Art. 11 Verbindliche unternehmensinterne Datenschutzvorschriften

[1] Verbindliche unternehmensinterne Datenschutzvorschriften nach Artikel 16 Absatz 2 Buchstabe e DSG gelten für alle Unternehmen, die zum selben Konzern gehören.

[2] Sie umfassen mindestens die in Artikel 9 Absatz 1 genannten Punkte sowie die folgenden Angaben:

a. die Organisation und die Kontaktdaten des Konzerns und seiner Unternehmen;
b. die innerhalb des Konzerns getroffenen Massnahmen zur Gewährleistung der Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften.

Neuer Vorschlag

[1] Verbindliche unternehmensinterne Datenschutzvorschriften nach Artikel 16 Absatz 2 Buchstabe e DSG gelten für alle verbundenen Unternehmen, die durch eine Kapital- oder Stimmenmehrheit unter einer einheitlichen Leitung zusammengefasst wurden.

[…]

Begründung

Es sollte genauer definiert werden, wann ein Unternehmen zum selben Konzern gehört. In der Regel wird von verbunden Unternehmen gesprochen, wenn eine Gesellschaft durch Kapital- oder Stimmenmehrheit eine oder mehrere Gesellschaften unter einheitlicher Leitung zusammenfasst.

Art. 13 Modalitäten der Informationspflichten

[1] Der Verantwortliche und der Auftragsbearbeiter teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit.

[2] Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.

Neuer Vorschlag

[1] Der Verantwortliche ~~und der Auftragsbearbeiter~~ teil~~ten~~ die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit.

[…]

[3] Der EDÖB stellt maschinenlesbare Piktogramme zur Verfügung.

Begründung

Betr. Abs. 1: Die Pflicht zur Information über die Beschaffung von Personendaten trifft nur den Verantwortlichen. Für eine Informationspflicht des Auftragsbearbeiters bei der Beschaffung besteht keine gesetzliche Grundlage.

Betr. Abs. 2: Es würde zur Standardisierung beitragen, wenn der EDÖB solche Icons zur Verfügung stellen würde.

Art. 15 Information bei der Bekanntgabe von Personendaten

Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.

Neuer Vorschlag

Art. 15 streichen.

Begründung

Eine Aussage über die Aktualität der Daten ist immer nur zutreffend im Zeitpunkt der Abgabe der Erklärung. Es ist oft unmöglich, die Zuverlässigkeit und Vollständigkeit der Daten zu gewährleisten.

Art. 18 Form und Aufbewahrung der Datenschutz-Folgenabschätzung

Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.

Neuer Vorschlag

Der Verantwortliche muss die Datenschutz-Folgenabschätzung in Textform festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.

Begründung

Es gibt keine gesetzliche Grundlage für eine Aufbewahrung in «Schriftform».

Art. 19 Meldung von Verletzungen der Datensicherheit

[1] Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit:

a. die Art der Verletzung;
b. soweit möglich den Zeitpunkt und die Dauer;
c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;
d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;
e. die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen;
f. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder die Folgen zu mildern;
g. den Namen und die Kontaktdaten einer Ansprechperson.

[2] Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

[3] Der Verantwortliche teilt den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mit.

[4] Handelt es sich beim Verantwortlichen um ein Bundesorgan, so erfolgt die Meldung an den EDÖB über die Datenschutzberaterin oder den Datenschutzberater.

[5] Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.

Neuer Vorschlag

[1] Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit im Sinne von Art. 24 Abs. 1 DSG:

[…]

f. welche Massnahmen getroffen wurden oder vorgesehen sind, um Risiken zu vermeiden, den Mangel zu beheben oder die Folgen zu mildern;

[3] Der Verantwortliche teilt den betroffenen Personen im Anwendungsbereich von Art. 24 Abs. 4 und 5 DSG in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mit.

Begründung

Betr. Abs. 1: Eine Meldepflicht gegenüber dem EDÖB besteht gem. Art. 24 Abs. 1 nDSG nur, wenn die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

Betr. lit. f: Es sollten auch Massnahmen getroffen werden, um die Risiken zu vermeiden.

Art. 20 Modalitäten

[1] Das Auskunftsbegehren wird schriftlich gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden.

[2] Die Auskunft wird in der Regel schriftlich erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat.

[3] Die Auskunft muss für die betroffene Person verständlich sein.

[4] Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.

[5] Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.

Neuer Vorschlag

[1] Das Auskunftsbegehren wird schriftlich oder auf elektronischem Weg gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden.

[2] Die Auskunft wird in der Regel schriftlich oder auf elektronischem Weg erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die betroffene Person kann hierbei auch kostenpflichtige Fotokopien bestimmter Akten verlangen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat.

[…]

Begründung

Der erläuternde Bericht hält fest, dass sowohl das Auskunftsbegehren als auch die –erteilung auf elektronischem Wege erfolgen kann. Dies sollte im Artikel ausdrücklich festgehalten werden.

Betr. Abs. 2: Gemäss erläuternder Bericht muss die betroffene Person bei der Einsichtnahme an Ort und Stelle die Möglichkeit haben, eine kostenpflichtige Fotokopie bestimmter Akten zu verlangen.

Art. 21 Zuständigkeit

[1] Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.

[2] Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen.

Neuer Vorschlag

Abs. 2 streichen.

Begründung

Damit erhalten Auftragsbearbeiter eine Pflicht, die im Gesetz so nicht vorgesehen ist. Zudem wäre so möglich, dass eine unkoordinierte Information an die betroffene Person erfolgt. Dies ist zu vermeiden, da dies nur zu Verwirrung führt.

Art. 23 Ausnahmen von der Kostenlosigkeit

[1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist.

[2] Die Beteiligung beträgt maximal 300 Franken.

[3] Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen.

Neuer Vorschlag

[2] Die Beteiligung beträgt die Hälfte des erwarteten angemessenen Aufwandes zu einem Ansatz eines kaufmännischen Mitarbeiters.

[3] Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen seit Mitteilung zurückziehen.

Begründung

Betr. Abs. 2: Die in Abs. 2 genannte Beteiligung entspricht nicht ansatzweise dem tatsächlichen Aufwand und ist dementsprechend anzupassen.

Betr. Abs. 3: Der Fristbeginn in Abs. 3 ist zu präzisieren.

Art. 25 Datenschutzberaterin oder Datenschutzberater

[1] Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen muss folgende Aufgaben wahrnehmen:

a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden.
b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.

[2] Der private Verantwortliche muss der Datenschutzberaterin oder dem Datenschutzberater:

a. die notwendigen Ressourcen zur Verfügung stellen;
b. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.

Neuer Vorschlag

Abs. 1 lit. b streichen.

Begründung

Betr. Abs. 1 lit. a: Die ist u.E. so zu belassen. Der Gesetzgeber hat im Gegensatz zur EU festgehalten, dass der Datenschutzberater anders als der Datenschutzverantwortliche nach DSGVO nicht nur eine Compliance- bzw. Kontrollfunktion hat, sondern eben auch den Datenschutz sicherstellen soll und selbst eingreifen kann und soll.

Betr. Abs. 1 lit. b: Die Litera ist zu streichen, da diese eine sinngemässe Wiederholung von Art. 23 Abs. 4 DSG darstellt, ohne zusätzliche Angaben zu machen.

Art. 26 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:

a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet.
b. Es wird ein Profiling mit hohem Risiko durchgeführt.

Neuer Vorschlag

Unternehmen und andere privatrechtliche Organisationen, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:

a. Es birgt ein Risiko für die Persönlichkeit oder Grundrechte der betroffenen Personen.

b. Die Bearbeitung erfolgt nicht nur gelegentlich.
c. Es werden besonders schützenswerte Personendaten bearbeitet.
d. Es wird ein Profiling mit hohem Risiko durchgeführt.

Begründung

Der Vorschlag ist nicht praktikabel und wirtschaftsfeindlich. Da eine Annäherung des Art. 26 an die Vorgaben der DSGVO wünschenswert ist, ist der Art. 26 dementsprechend anzupassen.

Art. 27 Ernennung

Jedes Bundesorgan ernennt eine Datenschutzberaterin oder einen Datenschutzberater. Mehrere Bundesorgane können gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater ernennen.

Neuer Vorschlag

[1] Jedes Bundesorgan ernennt eine Datenschutzberaterin oder einen Datenschutzberater. Mehrere Bundesorgane können gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater ernennen. Hierbei kann eine externe Datenschutzberaterin bzw. ein externer Datenschutzberater beauftragt werden.

Begründung

Es sollte dem Bundesorgan auch möglich sein, eine externe Datenschutzberaterin bzw. ein externer Datenschutzberater zu ernennen, da die Ressourcen auf dem Markt derzeit knapp sind.

Art. 28 Anforderungen und Aufgaben

[1] Die Datenschutzberaterin oder der Datenschutzberater muss die folgenden Anforderungen erfüllen:

a. Sie oder er verfügt über die erforderlichen Fachkenntnisse.
b. Sie oder er übt ihre oder seine Funktion gegenüber dem Bundesorgan fachlich unabhängig und weisungsungebunden aus.

[2] Sie oder er muss folgende Aufgaben wahrnehmen:

a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden.
b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese.
c. Sie oder er meldet dem EDÖB Verletzungen der Datensicherheit.
d. Sie oder er dient als Anlaufstelle für die betroffenen Personen.
e. Sie oder er schult und berät das Bundesorgan sowie dessen Mitarbeiterinnen und Mitarbeiter in Fragen des Datenschutzes.

Neuer Vorschlag

Art. 28 Anforderungen und Aufgaben des Datenschutzberaters für Bundesorgane

[…]

Begründung

Es ist notwendig den Titel von Art. 28 zu präzisieren, da man prima vista sonst annehmen könnte, es handle sich um die Aufgaben des Beraters für Unternehmen.

Art. 31 Information an die Datenschutzberaterin oder den Datenschutzberater

Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von Personendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden.

Neuer Vorschlag

Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von besonders schützenswerten Personendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden.

Begründung

Eine generelle Bewilligungspflicht von Projekten entspricht nicht dem Willen des Gesetzgebers, weswegen die Bewilligungspflicht auf die automatisierte Bearbeitung von besonders schützenswerten Personendaten zu beschränken ist.

Art. 33 Unentbehrlichkeit der Testphase

Eine Testphase als Pilotversuch ist unentbehrlich, wenn eine der folgenden Bedingungen erfüllt ist:

a. Die Erfüllung einer Aufgabe erfordert technische Neuerungen, deren Auswirkungen zunächst evaluiert werden müssen.
b. Die Erfüllung einer Aufgabe erfordert bedeutende organisatorische oder technische Massnahmen, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit zwischen Organen des Bundes und der Kantone.
c. Die Erfüllung der Aufgaben erfordert, dass die Personendaten mittels eines Abrufverfahrens zugänglich gemacht werden.

Neuer Vorschlag

Eine Testphase als Pilotversuch ist unentbehrlich, wenn sie zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt und eine der folgenden Bedingungen erfüllt ist: […]

Begründung
Die Testphase als Pilotversuch ist an ein erhöhtes Risiko für betroffene Person zu knüpfen.

Art. 41 Selbstkontrolle
[1] Der EDÖB erstellt ein Bearbeitungsreglement für sämtliche automatisierten Bearbeitungen. Artikel 5 Absatz 1 findet keine Anwendung.

[2] Er sieht interne Prozesse vor, die gewährleisten, dass die Bearbeitungen entsprechend dem Bearbeitungsreglement vorgenommen werden. Er überprüft jährlich, ob das Bearbeitungsreglement eingehalten wird.

Neuer Vorschlag
[1] Der EDÖB erstellt ein Bearbeitungsreglement für sämtliche automatisierten Bearbeitungen innerhalb seiner Behörde. Artikel 5 Absatz 1 findet keine Anwendung.

Begründung
Abs. 1 ist im Sinne der Ausführungen im erläuternder Bericht zu präzisieren.

[…]

Nach dem Gesagten danken wir Ihnen, sehr geehrte Frau Bundesrätin Keller-Sutter, sehr geehrter Herr Amstutz, sehr geehrte Damen und Herren, bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für allfällige Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Nicole Beranek Zanon
PARTNERIN

LAW FIRM
ÉTUDE D'AVOCATS

Département fédéral de justice et police
DFJP
jonas.amstutz@bj.admin.ch

Lausanne, le 1er septembre 2021

Projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Madame la Conseillère fédérale,
Mesdames, Messieurs,

Dans le délai imparti au 14 octobre 2021, les deux soussignés ont le plaisir de participer spontanément et à titre personnel à la consultation mentionnée sous rubrique.

Les exigences minimales en matière de sécurité des données (art. 1 et 2 P-OLPD)
Le principe de la sécurité des données personnelles, exprimé à l'art. 8 nLPD, est l'un des points cardinaux du traitement de données personnelles, et celui qui ne respecte pas les exigences minimales en matière de sécurité prévues dans l'OLPD réalise entre autres une infraction pénale, passible d'une amende jusqu'à CHF 250'000.- (art. 8 al. 3 et 61 nLPD).

Malgré le caractère essentiel de ce principe, le P-OLPD laisse une grande liberté dans l'identification et l'application des mesures techniques et organisationnelles devant concrètement être mises en œuvre afin justement de le respecter. Il prévoit uniquement des objectifs qui doivent « dans la mesure du possible » être atteints par les mesures prises (art. 2). Quant à l'art. 1, il indique une série de critères à prendre en compte pour évaluer si les mesures sont adaptées aux risques.

Pourtant, le droit pénal obéit au principe de légalité (*nullum crimen, nulla pœna sine lege*). L'art. 1 CP rappelle au besoin qu'une peine ou une mesure ne peuvent être prononcées qu'en raison d'un acte expressément réprimé par la loi.

Av. Auguste Tissot 2bis
Case postale 851
CH-1001 Lausanne
T +41 (0)21 310 73 10
F +41 (0)21 310 73 11
@hdclegal
www.hdclegal.ch

En l'espèce, le P-OLPD ne permet pas de définir avec suffisamment de précision l'absence de quelle mesure précise réaliserait une infraction pénale. Il est donc nécessaire de détailler les mesures minimales.

L'obligation de journalisation (art. 3 P-OLPD)

L'obligation de journalisation s'applique au responsable du traitement privé et à son sous-traitant en cas de risque résiduel élevé (indépendamment d'un traitement automatisé), alors qu'elle s'applique à l'organe fédéral et à son sous-traitant en cas de traitement automatisé (indépendamment d'un risque résiduel). Tant cette distinction en général, que le régime choisi pour le responsable du traitement privé en particulier, ne doivent pas être confirmés dans la version finale de l'OLPD.

Premièrement, la notion de « traitement automatisé » n'est pas définie dans la nLPD ou l'OLPD, alors qu'elle est déjà utilisée dans la définition du profilage (art. 5 let. f nLPD) et pourrait être comprise comme proche d'autres concepts prévus dans la nLPD, dont les décisions individuelles automatisées (art. 21 nLPD) ou les essais pilotes menés justement sur des traitements de données personnelles automatisées (art. 35 nLPD). Elle peut aussi être comprise largement et viser la plupart des traitements informatiques (qui incluent une logique automatique de traitement de la donnée).

Deuxièmement, si l'exigence de journalisation se comprend et est bienvenue en cas de traitement automatisé avec un risque résiduel, ainsi que dans le cadre de la Directive 2016/680, une application systématique est disproportionnée et risque d'être particulièrement difficile à respecter. Elle représente un risque de surveillance massive des personnes concernées et l'on peut sérieusement se demander si tous les outils informatiques du marché (y compris les outils de traitement de texte de base), permettent réellement de savoir qui a consulté et quand une partie d'un texte.

Troisièmement, l'obligation de journalisation sera en pratique très difficile à respecter, en tout cas intégralement. Or, ce non-respect pourrait constituer une infraction pénale selon l'art. 61 let. c nLPD en tant que la journalisation intègre les exigences minimales en matière de sécurité. En conséquence, cette situation mènera vraisemblablement à de nombreuses violations pénales théoriques, qui resteront non-poursuivies vu leur nombre. Quelque chose qu'il convient impérativement d'éviter.

Cette obligation doit être limitée aux cas représentant un risque résiduel élevé et où la mesure est adaptée au sens de l'art. 1 P-OLPD.

Le règlement de traitement (art. 4 et 5 P-OLPD)

La LPD prévoit un « règlement de traitement » à l'art. 36 LPD et la possibilité de déterminer par voie d'ordonnance les fichiers dont le traitement devant en faire l'objet. L'art. 12 nLPD a cependant introduit la notion de « registre des traitements » et, en conséquence, ne prévoit plus l'obligation d'avoir un règlement de traitement. En

conséquence, la conservation d'une telle obligation dans le cadre du P-OLPD ne paraît pas conforme au principe de la base légale suffisante. Ceci *a fortiori* dans la mesure où les art. 1 et 2 P-OLPD ne détaille pas le règlement de traitement comme une mesure imposée.

La sous-traitance (art. 6 et 7 P-OLPD)
L'exigence d'une autorisation écrite pour la délégation de deuxième rang est bienvenue, mais elle ne figure pas dans la nLPD. On peut donc se demander si elle peut réellement être imposée aux organes fédéraux qui ne sont pas soumis à la Directive 2016/680.

L'obligation d'informer le conseiller à la protection des données prévue à l'art. 7 est intéressante, mais on peine à voir son rattachement dans la nLPD. Surtout, il est difficile de percevoir les conséquences de sa violation, notamment si cela rend le traitement illicite et si une personne concernée pourrait faire valoir des prétentions sur cette base (art. 41 nLPD).

Spécifiquement sous l'angle de l'art. 6 al. 2 P-OLPD, l'application du critère large des effets figurant à l'art. 3 nLPD rend peu probable qu'un sous-traitant ne soit pas soumis à la LPD de façon générale.

La communication à l'étranger (art. 8 à 12 OLPD)
L'art. 8 P-OLPD introduit la possibilité de reconnaître un territoire, un État fédéré ou un « secteur déterminé » comme adéquat, alors que la loi ne prévoit pas une telle granularité et se contente d'un État ou d'un organisme international. L'approche est intéressante, mais *ultra legem*. Il peut en revanche s'agir d'une autre garantie (au sens de l'art. 16 al. 3 nLPD). Si le principe de la possibilité de reconnaître un secteur déterminé relève de la compétence du Conseil fédéral, il ne s'agit ensuite pas d'une décision d'adéquation du Conseil fédéral mais au contraire de garanties à communiquer préalablement au PFPDT (sans que ce dernier ne doive les approuver). La notion de secteur déterminé n'est en outre pas définie, ce qui pose évidemment des risques dans l'interprétation et l'application.

Le respect des droits humains, aussi noble soit-il, n'est pas un critère pertinent. Soit la protection de la personnalité est garantie (et les droits humains qui y sont liés sont déjà respectés), soit elle ne l'est pas. Au surplus, la notion de droits humains fait probablement référence aux droits fondamentaux (art. 7 ss Cst.) et on voit mal pourquoi un État qui autoriserait la dissimulation du visage dans l'espace public ou ne garantirait pas la liberté de l'art ou le droit à un enseignement de base gratuit ne pourrait pas être adéquat.

L'art. 8 P-OLPD devrait préciser que le niveau jugé adéquat est celui qui correspond à la nLPD (ce qui peut être un niveau inférieur à celui exigé par d'autres législations ou autorités).

La procédure d'évaluation n'est pas réglée, en particulier comment un État (et cas échéant un secteur déterminé) peut demander une décision et si celle-ci est sujette à recours. Les critères établis sont juridiques et ne laissent pas la place à une opportunité de rendre ou non une décision en cas de demande. On peut aussi se demander si un exportateur de données pourrait prétendre à un intérêt digne de protection et demander qu'une décision soit rendue. Il convient donc de préciser ces éléments et prévoir ou exclure, cas échéant, une qualification explicite de décision sujette à recours. Dans ce dernier cas, la voie de recours devrait être précisée.

La communication facultative (art. 14 P-OLPD)
Cette disposition rappelle le principe de l'autodétermination informationnelle, la demande d'un organe fédéral laissant penser que la communication est nécessaire. Son caractère facultatif devrait être indiqué dans tous les cas, et pas seulement dans le cas du recours à un questionnaire lors d'une collecte systématique.

L'actualité, la fiabilité et l'exhaustivité des données (art. 15 P-OLPD)
Cette exigence paraît particulièrement difficile à réaliser et devrait être limitée aux données pour lesquelles le traitement représente un risque résiduel. Elle ne se retrouve par ailleurs pas dans la nLPD, de sorte qu'elle pourrait sortir du cadre des art. 19 ss nLPD.

L'information sur la rectification, l'effacement, etc. (art. 16 P-OLPD)
Ces obligations devraient être limitées dans le temps. Il faut aussi préciser que cela ne constitue pas une obligation pour le responsable du traitement de conserver une copie des données communiquées et des destinataires y relatifs.

Le réexamen d'une décision individuelle automatisée (art. 17 P-OLPD)
La portée de l'interdiction prévue à l'art. 17 P-OLPD devrait être précisée et clarifiée. En l'état en effet, il n'est pas clair de savoir si cette interdiction porte sur l'impossibilité pour le responsable du traitement de revenir sur sa décision au détriment de la personne concernée après analyse par une personne physique, y compris en en cas d'erreur constatée, ou si elle ne concerne que l'interdiction de refuser un service précédemment fourni à la personne concernée au seul motif qu'elle a demandé un réexamen de la décision automatisée.

Analyse d'impact relative à la protection des données personnelles (art. 18 P-OLPD)
L'imposition de la forme écrite ne se justifie pas. Pour rappel, la forme écrite exige une signature (TAF A-3548/2018). Il devrait également être possible d'établir et conserver l'analyse d'impact en la forme électronique – toujours à la condition qu'elle soit conservée de façon sécurisée et puisse immédiatement être retrouvée. Si la forme écrite de l'analyse d'impact devait néanmoins être maintenue, elle doit nécessairement être comprise de façon plus large que la règle formelle (et contractuelle) des art. 12 ss CO ; un point qu'il est nécessaire de spécifiquement prévoir.

Les violations de la sécurité des données (art. 19 P-OLPD)
L'art. 24 nLPD ne prévoit pas d'obligation de documenter et conserver les informations liées à une violation de sécurité. Cela est d'autant plus surprenant que l'obligation s'applique à toutes les violations de sécurité, y compris celles qui ne justifient pas d'annonce.

L'art. 24 al. 6 nLPD prévoit qu'une annonce ne peut être utilisée dans le cadre d'une procédure pénale contre la personne tenue d'annoncer qu'avec son consentement. Il serait utile de préciser que la personne tenue d'annoncer est, dans le cas d'une personne morale, la personne morale en tant que telle et toute personne physique en son sein tenue d'annoncer.

Le droit d'accès (art. 20 ss P-OLPD)
Si les deux parties sont d'accord, la consultation sur place doit pouvoir avoir lieu indépendamment de savoir qui l'a proposée.

L'exigence de la forme écrite ne se justifie pas dans tous les cas, la forme électronique peut généralement être suffisante. Rien ne justifie que le responsable du traitement ait besoin d'une signature manuscrite en lien avec la demande d'accès s'il n'en avait pas connaissance avant (par exemple un compte en ligne).

Il faudrait préciser que le délai de 30 jours court dès la réception de la demande ou, cas échéant, de la confirmation de l'acception des frais. La personne concernée ne devrait pas seulement pouvoir retirer sa demande pendant 10 jours, elle devrait au contraire confirmer sa demande en acceptant les éventuels frais. L'absence de réponse, ou une réponse tardive, sont problématiques pour le responsable du traitement qui doit précisément déployer des efforts disproportionnés sans obtenir de garantie quant au paiement.

Finalement, la notion de demande de renseignements ne correspond pas à la nLPD.

La remise ou à la transmission des données personnelles (art. 24 P-OLPD)
L'art 28 nLPD prévoit que la personne concernée peut demander au responsable du traitement la remise ou à la transmission des données personnelles la concernant si les données personnelles sont traitées avec son consentement ou en relation directe avec la conclusion ou l'exécution d'un contrat. Cette formulation malheureuse est reprise du RGPD, qui exige en tout temps un motif justificatif, mais ne correspond pas à l'esprit de la nLPD ni au système qui y est mis en place. Littéralement, des données traitées sans atteinte la personnalité au sens de l'art. 30 nLPD (et donc sans consentement ou contrat) ne peuvent pas faire l'objet d'un droit à la remise, alors qu'en cas d'atteinte ce droit serait ouvert.

L'ordonnance devrait corriger ce point.

L'exception au registre (art. 26 P-OLPD)
Cette exception doit être saluée.

Il faudrait encore préciser que si l'une des conditions est remplie, l'obligation de tenir un registre s'applique seulement pour les traitements concernés et pas pour l'ensemble des traitements et données.

Collaboration avec le NCSC (art. 42 P-OLPD)
L'art. 42 al. 1 P-LPD parle de la personne responsable de l'annonce, ce qui se rapproche de la notion de personne tenue d'annoncer de l'art. 24 al. 6 nLPD, alors qu'il faudrait simplement mentionner le responsable du traitement.

Le représentant (art. 14 s nLPD)
La disposition sur le représentant a été ajoutée par le parlement. On ne trouve donc aucune information dans le Message du Conseil fédéral. Il pourrait être utile de préciser dans l'OLPD l'absence de responsabilité subsidiaire du représentant (tant sous l'angle civil que pénal). L'obligation de tenir un registre crée en effet une incertitude, notamment pour les manquements qui seraient imputable au responsable du traitement. En outre, les modalités de sa désignation ainsi que les éventuelles connaissances dont il devrait bénéficier devraient aussi être précisées.

Veuillez croire, Madame la Conseillère fédérale, Mesdames, Messieurs, à l'expression de ma parfaite considération

Sylvain Métille
Professeur ass., Dr jur, avocat
metille@hdclegal.ch

David Raedler
Dr jur, avocat
raedler@hdclegal.ch

beider basel
handelskammer

Frau Bundesrätin
Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement
EJPD
Bundeshaus West
3003 Bern
Ausschliesslich per E-Mail an:
jonas.amstutz@bj.admin.ch

Basel, 13. Oktober 2021 pho

Stellungnahme zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit, uns in rubrizierter Angelegenheit äussern zu können. Die Handelskammer beider Basel setzt sich für einen modernen und zweckmässigen Datenschutz ein, der die Innovationskraft unseres Landes und insbesondere unserer Region Basel nicht behindert.

In der Anlage finden Sie unsere Stellungnahme.

Für die Kenntnisnahme danken wir Ihnen und bitten Sie, unsere Überlegungen für die weiteren Arbeiten zu berücksichtigen.

Freundliche Grüsse

Handelskammer beider Basel Handelskammer beider Basel

Martin Dätwyler
Direktor

Deborah Strub
Abteilungsleiterin Cluster & Initiativen
Mitglied der Geschäftsleitung

Beilage: Stellungnahme

Martin Dätwyler
Direktor

T +41 61 270 60 81
F +41 61 270 60 05

m.daetwyler@hkbb.ch

Handelskammer beider Basel
St. Jakobs-Strasse 25
Postfach
CH-4010 Basel

T +41 61 270 60 60
F +41 61 270 60 05

www.hkbb.ch

beider basel handelskammer

Stellungnahme

Basel, 13. Oktober 2021 pho

zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Die Handelskammer beider Basel beantragt eine ausführliche Überarbeitung des Entwurfes der Verordnung zum Bundesgesetz über den Datenschutz. Der Entwurf der totalrevidierten Verordnung zum DSG (E-VDSG) folgt der vom Parlament im revDSG vorgegebenen Stossrichtung nicht. Er verschärft wesentliche Punkte des Gesetzes, ist inhaltlich nicht ausreichend präzise und unnötig restriktiv. Statt das revDSG im Sinne von Ausführungsvorschriften zu konkretisieren, sieht die Verordnung eine Reihe von bürokratischen Zusatzvorschriften mit vielen «Swiss Finishes» vor, die keine Grundlage im Gesetz finden. Die Verordnung stellt keine Grundlage für einen zweckmässigen, zukunftsgerichteten Datenschutz dar.

Ausgangslage

Die Handelskammer beider Basel setzt sich für einen modernen und zweckmässigen Datenschutz ein, der die Innovationskraft unseres Landes nicht behindert. In einer zunehmend digitalisierten Wirtschaft ist es von grundsätzlicher Bedeutung, dass die Datenschutzgesetzgebung eine die Innovationskraft des Standortes Schweiz und insbesondere der Region Basel nicht beeinträchtigende Balance zwischen einem angemessenen Schutz der Daten und der wirtschaftlichen Nutzung von Daten findet. Ein administrativ tragbares Vorgehen im Rahmen der internationalen Entwicklungen ist dabei zentral. Im Zentrum stand bereits bei der parlamentarischen Beratung zum revidierten Datenschutzgesetz die Eingliederung in diese Entwicklungen; Schweizer Besonderheiten wurden dabei grösstenteils vermieden. Mit dem revDSG konnte im Herbst 2020 ein modernes Gesetz geschaffen werden, welches das Schutzniveau der DSGVO übernimmt, die Anliegen der Politik und Wirtschaft angemessen berücksichtigt und zahlreiche Verbesserungen gegenüber dem bisherigen DSG beinhaltet.

Vorlage

Der Entwurf der totalrevidierten Verordnung zum DSG (E-VDSG) folgt der vom Parlament im revDSG vorgegebenen Stossrichtung nicht. Er verschärft wesentliche Punkte des Gesetzes, ist inhaltlich nicht ausreichend präzise und unnötig restriktiv. Statt das revDSG im Sinne von Ausführungsvorschriften zu konkretisieren, sieht die Verordnung eine Reihe von bürokratischen Zusatzvorschriften mit vielen «Swiss Finishes» vor, die keine Grundlage im Gesetz finden.

Handelskammer beider Basel
St. Jakobs-Strasse 25
Postfach
CH-4010 Basel

T +41 61 270 60 60
F +41 61 270 60 05

www.hkbb.ch

Die Verordnung wirkt wie ein unabhängig vom revDSG entstandenes Regelwerk. Die politischen Diskussionen und Erwägungen der DSG-Debatte wurden nicht ausreichend berücksichtigt. Dieses Problem zeigt sich sowohl in der Verordnung wie auch im Erläuterungsbericht. Der Entwurf muss unter Berücksichtigung des revDSG und insbesondere der politisch intensiv geführten Diskussion, welche zu zahlreichen Kompromissen im Parlament geführt hat, nochmals stark verbessert werden.

Der vorliegende Entwurf wird von der Handelskammer beider Basel abgelehnt. Er stellt keine Grundlage für einen zweckmässigen, zukunftsgerichteten Datenschutz dar.

Unsere Forderungen

Gestützt auf obgenannte Ausgangslage stellen wir daher die Forderung, die Revisionsvorlage bzw. den Entwurf mitsamt Erläuterungsbericht einer ausführlichen Überarbeitung zu unterziehen. Dies unter Respektierung der Kohärenz zum revDSG und einer Verhinderung von «Swiss Finishes» und unnötigen Restriktionen. Diese Überarbeitung muss unter Einsetzung der notwendigen Ressourcen zeitnah erfolgen, damit die Äquivalenz aufrechterhalten werden kann. Im Weiteren verweisen wir auf die ausführliche Stellungnahme von economiesuisse.

HotellerieSuisse

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Bern, 06.10.2021

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz: Stellungnahme anlässlich der Vernehmlassung

Sehr geehrte Frau Bundesrätin,
sehr geehrter Herr Amstutz

Als nationaler Unternehmerverband äussert sich HotellerieSuisse im Rahmen des Vernehmlassungsverfahrens zur totalrevidierten Datenschutzverordnung. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Anliegen.

1. Grundsätzliches

HotellerieSuisse unterstützt als Verband der innovativen und nachhaltigen Beherbergungsbetriebe die mit der Revision der VDSG verfolgten Ziele (Anpassung an die revidierten Vorgaben im revDSG und den europäischen Bestimmungen, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig möglich bleibt). Die datenschutzrechtlichen Bestimmungen der Datenschutz-Grundverordnung (DSGVO), Richtlinie EU 2016/680 und der revidierten Übereinkommen SEV 108 des Europarats betreffen auch viele Schweizer Beherbergungsbetriebe. HotellerieSuisse kann die Umsetzung gemäss aktuell vorliegendem Entwurf nicht unterstützen Die Stossrichtung des Entwurfs bezüglich der neu vorgesehenen Dokumentations- und Informationspflichten geht viel zu weit, schafft zusätzliche unnötige administrative Aufwände und schiesst in der Gesamtheit betrachtet übers Ziel hinaus, insbesondere dort, wo diese neuen Pflichten überhaupt keine Grundlage im revDSG haben oder bereits während dem Revisionsverfahren des revDSG verworfen wurden.

HotellerieSuisse ist der Ansicht, dass die Regelungen des E-VDSG – als Ausführungsverordnung zum revidierten Datenschutzgesetz (Erläuternder Bericht, BJ, Ziffer 1.4, S. 9) – lediglich die gesetzlichen Bestimmungen des revDSG konkretisieren können, nicht aber darüber hinausgehen, unnötig ausweiten oder gar neue Verpflichtungen einführen dürfen. Das gilt besonders für Regelungen des Entwurfs, die keine Detailvorschriften sind, sondern in ihrer Bedeutung den in der revDSG enthaltenen Bestimmungen gleichkommen. Auf zusätzliche eigene Regelungen und zusätzliche «Swiss Finishs» ist in der E-VSDG zwingend zu verzichten, insbesondere wenn deren Grundzüge nicht bereits in der re-

HotellerieSuisse, Monbijoustrasse 130, Postfach, CH-3001 Bern
T +41 31 370 41 11, welcome@hotelleriesuisse.ch, www.hotelleriesuisse.ch

vDSG festgehalten sind – und somit keine gesetzliche Grundlage besteht. Diese vorgesehenen, zusätzlichen Regelungen vereiteln das Ziel der Revisionen von DSG und VDSG. Bei den vorgesehenen Informations- und Dokumentationspflichten muss zwingend auf eine Überregulierung verzichtet werden. Dokumentations- und Informationspflichten, welche bereits im Rahmen der Vernehmlassung zum revDSG verworfen wurden, dürfen aus unserer Sicht keinen Einzug in die Verordnung halten und sind klar abzulehnen.

Angesichts dessen, dass die «Angemessenheit» des Schutzes gemäss DSGVO wie gesagt lediglich einen «angemessenen» Schutz durch Rechtsstaatlichkeit, gelebte Schutzmechanismen, Betroffenenrechte und unabhängige Aufsicht verlangt (Art. 45 Abs. 2 DSGVO), ist auf jegliche weitergehende Verschärfung in der schweizerischen Gesetzgebung zu verzichten, um die ohnehin schon entstehenden zusätzlichen Kosten und neuen administrativen Aufwände auf das Nötigste begrenzt zu halten.

2. Zu den Einzelnen Bestimmungen:

➔ Art. 1 E-VDSG – Grundsätze

Bei der Beurteilung der Angemessenheit der Massnahmen sind gemäss Art. 1 Abs. 1 lit. d E-VDSG die Implementierungskosten ein massgebendes Kriterium. Es sind aber nicht nur die Implementierungskosten an sich, sondern der generelle Implementierungsaufwand relevant (insb. personelle, strukturelle oder organisatorische Aufwendungen). Dieser Gesamtaufwand der einzelnen Massnahmen sollte in die Beurteilung einfliessen. Die Erläuterungen im Bericht (vgl. S. 16) sind betreffend die Berücksichtigung der Implementierungskosten dann auch zu restriktiv. Die Kosten resp. der Aufwand müssen bereits bei der Beurteilung der Massnahmen und deren Angemessenheit an sich berücksichtigt werden können und nicht erst, wenn es darum geht, aus verschiedenen zur Verfügung stehenden Massnahmen, die günstigste auswählen zu dürfen. Logischerweise wird der oder die Verantwortliche aus den zur Verfügung stehenden und angemessenen Massnahmen in der Regel die kostengünstigste Variante auswählen.

Empfehlung:

Art. 1 E-VDSG: 1 *«Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:*

a. Zweck, Art, Umfang und Umstände der Datenbearbeitung;
b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen;
c. der Stand der Technik;
d. Implementierungs~~kosten~~aufwand.»

➔ Art. 3 E-VDSG – Protokollierung

Die Protokollierungspflicht nach Art. 3 E-VDSG hat keine gesetzliche Grundlage im revDSG und stellt ein zusätzliches «Swiss Finish» dar. Auch die DSGVO sieht keine Protokollierungspflicht für Privatpersonen vor. Art. 3 Absatz 2 E-VDSG richtet sich an die Bundesorgane und ist nicht auf Privatpersonen anwendbar. Zudem wurde bereits im Rahmen der Vernehmlassung zur revDSG auf eine Protokollierungspflicht verzichtet und eine Einführung durch die Hintertür auf Verordnungsebene wird klar abgelehnt. Demgegenüber fand die Pflicht zur Führung eins Verzeichnisses der Bearbeitungstätigkeiten gemäss Art. 12 revDSG Einzug im Gesetz. In diesen Verzeichnissen

müssen alle Datenbearbeitungstätigkeiten festgehalten werden, entsprechend ist das Führen eines Protokolls obsolet und die Bestimmung – zumindest für den privaten Bereich – zu streichen.

Empfehlung: Art. 3 E-VDSG: Streichen für den privaten Bereich

➔ **Art. 4 E-VDSG – Bearbeitungsreglement von privaten Personen**

Die Meldepflicht für private Verantwortliche gemäss Art. 11a aDSG besteht im revDSG nicht mehr, womit auch die Verpflichtung ein Bearbeitungsreglement erstellen zu müssen, mangels Grundlage entfällt. Art. 8 Abs. 3 revDSG, welcher als Grundlage für die Verordnungsbestimmung dienen soll, äussert sich nicht zum Bearbeitungsreglement als Element der Mindestanforderungen für die Datensicherheit. Bereits in der Botschaft zum revDSG (BBl 2017 6978, Ziff, 1.6.2.1) wurde festgehalten, dass *«anstelle einer allgemeinen Dokumentationspflicht […] eine Bestimmung über ein Verzeichnis der Bearbeitungstätigkeiten eingefügt wurde»*. Folglich genügt zur Dokumentation ein Bearbeitungsverzeichnis gemäss Art. 12 revDSG. Auch die DSGVO sieht keine Pflicht zur Erstellung eines Reglements vor. Dieses «Swiss Finish» ist zu streichen.

Weiter suggeriert die im Entwurf gefasste Version von Art.4 Abs. 3 E-VDSG, dass in jedem Fall ein Datenschutzberater zu bestellen ist. Das ist aber bei Privaten nur optional, selbst wenn nach dem Entwurf ein Bearbeitungsreglement zu führen wäre.

Empfehlung: Streichung von Art. 4 E-VDSG

➔ **Art. 6 E-VSDG – Modalitäten**

Art. 6 Abs. 1 E-VDSG, 2ter Satz

Gemäss erläuterndem Bericht (S. 23 f.) präzisiert der zweite Satz von Art. 6 Abs. 1 E-VDSG die Verantwortlichkeit, wenn die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen wurde. Die Sicherstellung, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden, ist aber dem Verantwortlichen in dieser Situation nicht (mehr) möglich. Sobald die Datensätze einem Auftragsbearbeiter übertragen sind, liegt die Sicherstellung der Datensicherheit nicht mehr im Einflussbereich des oder der Verantwortlichen, resp. ist dessen bzw. deren Einflussnahme stark eingeschränkt. Vielmehr sollten die Verantwortlichen dazu verpflichtet werden, nur Auftragsbearbeiter zu beauftragten, welche durch angemessene Massnahmen (bspw. durch Massnahmen nach Art. 2 E-VSDG) die Anforderungen des revDSG in Bezug auf die Gewährleistung der Datensicherheit und den Schutz der Rechte der Betroffenen einhalten können – oder Garantie(n) dafür bieten. Eine solche Regelung entspricht Art. 28 DSGVO.

Alternativ ist die Sicherstellung der vertrags- oder gesetzesgemässen Bearbeitung durch eine schriftliche Verpflichtung der Auftragsbearbeiter zu erreichen.

Empfehlung 1: Art. 6 Abs. 1 E-VDSG: *1 «Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich~~. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.~~ Er arbeitet nur mit Auftragsbearbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.»*

Eventualiter: Art. 6 Abs. 1 E-VDSG: *1 «Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich~~. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.~~ Er stellt die vertrags- oder gesetzesgemäss Datenbearbeitung durch den Auftragsbearbeiter auf vertraglichem Weg sicher.»*

Erläuternder Bericht, S. 24, zu Art. 6 E-VDSG

Der erläuternde Bericht hält in Bezug auf Art. 6 E-VDSG Mindestvorgaben der in einem Vertrag oder im Gesetz zu regelnden Aspekten fest (vgl. Seite 24). Diese entsprechen den Vorgaben von Artikel 22 Absatz 3 der Richtlinie (EU) 2016/680. Das suggeriert, dass diese inhaltlichen Anforderungen auch gemäss E-VDSG gelten. Hierfür finden sich allerdings keine gesetzlichen Grundlagen und der Erläuterungsbericht ist zu korrigieren. Entsprechend ist im erläuternden Bericht festzuhalten, dass die E-VDSG keine Mindestanforderungen an die vertraglichen und/oder gesetzlichen Regelungen vorschreibt.

➔ **Art. 9 Abs. 2 E-VDSG – Datenschutzklauseln und spezifische Garantien und Art. 10 Abs. 1 E-VDSG – Standarddatenschutzklauseln**

Die Verpflichtung des Verantwortlichen, angemessene Massnahmen zu treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln und spezifischen Garantien (Art. 9 Abs. 2 E-VDSG) oder Standarddatenschutzklauseln (Art. 10 Abs. 1 E-VDSG) einhält resp. beachtet, geht zu weit. Es muss ausreichend sein, dass der Verantwortliche den Empfänger oder die Empfängerin schriftlich zur Einhaltung der Datensicherheit und der Rechte der Betroffenen in der Datenschutzklausel und spezifischen Garantien sowie der Standarddatenschutzklauseln verpflichtet oder aber, dass eine solche schriftliche Verpflichtung in den genehmigten Standarddatenschutzklauseln selbst enthalten ist.

Sobald die Datensätze ins Ausland übertragen wurden, kann der Verantwortliche nicht «sicherstellen», dass die Datenschutzklauseln in einem Vertrag, die spezifischen Garantien oder die Standarddatenschutzklauseln von dem Empfänger oder der Empfängerin eingehalten werden. Er kann aber, bspw. durch vertragliche Verpflichtungen, – u.a. unter Androhung von Konsequenzen bei Nichteinhalten dieser – anstrengen, dass die Empfänger diese einhalten bzw. beachten.

Weiter sind die zu treffenden Massnahmen zur Gewährleistung der Datensicherheit gemäss Art. 9 Abs. 1 lit. h. E-VDSG bereits in den Datenschutzklausel oder spezifischen Garantien selbst festzuhalten. Dies betrifft sowohl die Datenübermittlung als auch die Bearbeitung der Datensätze durch die Empfängerin oder den Empfänger. Gemäss Erläuterungsbericht bezieht sich die Angemessenheit der geforderten Massnahmen von Art. 9 Abs. 2 E-VDSG – wie schon jene unter Art. 9 Abs. 1 lit. h. E-VDSG – nach den Umständen im konkreten Fall und dem Stand der Technik. Daher ist die erneute Verpflichtung des Verantwortlichen angemessene Massnahmen zu treffen, um die Einhaltung der Datenschutzklauseln sicherzustellen, redundant. Dies sollte vielmehr durch die schriftliche Verpflichtung der Empfängerin oder des Empfängers zur Einhaltung resp. Beachtung der Datenschutzklauseln erreicht werden. Im Falle von Art. 10 Abs. 1 E-VSDG kann zudem festgehalten werden, dass diese Bestimmung durch die Einführung der neuen Standardvertragsklauseln eigentlich überflüssig geworden ist.

Empfehlung 1: Art. 9 Abs. 2 E-VDSG: *2 «~~Der Verantwortliche muss angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.~~ Der Verantwortliche verpflichtet die*

Empfängerin oder den Empfänger schriftlich zur Einhaltung der Datenschutzklauseln oder der spezifischen Garantien und der Rechte der Betroffenen»

Empfehlung 2: Streichung von Art. 10 Abs. 1 E-VDSG

Eventualiter: Art. 10 Abs. 1 E-VDSG: «*Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt,* ~~*so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.*~~ *so verpflichtet er die Empfängerin oder de*~~*r*~~*n Empfänger diese zu beachten.*»

➔ **Art. 13 E-VDSG – Modalitäten der Informationspflichten**

In Art. 19 Abs. 1 revDSG wird nur der Verantwortliche zur Information bei der Beschaffung von Personendaten verpflichtet. Dass nun im Entwurf der Verordnung die Informationspflicht ebenfalls auf den Auftragsbearbeiter oder die Auftragsbearbeiterin ausgeweitet wird, entbehrt der gesetzlichen Grundlage und ist zu streichen. Ggf. sind die dazugehörigen Passagen im erläuternden Bericht zu korrigieren (vgl. Ziffer 4.2, S. 30).

Empfehlung: Art. 13 Abs. 1 E-VDSG: *1 «Der Verantwortliche* ~~*und der Auftragsbearbeiter teilen*~~ *teilt die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht* zugänglicher Form mit.»

Erläuternder Bericht (S. 30)

Art. 19 Abs. 1 revDSG hält fest, dass der Verantwortliche die betroffenen Personen «angemessen» über die Beschaffung von Personendaten informieren muss. Entsprechend kommt es bei der Mitteilung auf die konkreten Umstände der Einzelfälle drauf an. Mitunter ist auch das Informationsinteresse der betroffenen Person zu berücksichtigen.

Die Ausführungen im erläuternden Bericht zu Art. 13 Abs. 1 E-VSDG vermitteln aber eine weitaus strengere Regelung betreffend diese Informationspflicht. Der Verantwortliche soll «*bei der Wahl der Informationsform sicherstellen, dass die betroffene Person die wichtigsten Informationen stets auf der ersten Kommunikationsstufe erhält*». Eine solche Handhabe wäre überbordend, zumal der Begriff der «wichtigsten Informationen» nicht genügend bestimmt ist. Auch ist nicht klar, ob damit die «Basisinformationen», wie sie in der DSGVO genannt werden, gemeint sind. In einer reinen Online-Umgebung, welche im Erläuternden Bericht als Beispiel aufgeführt wurde, mag die Informationspflicht einfach umzusetzen sein. Im alltäglichen Geschäftsverkehr (Telefon- oder E-Mail-Verkehr, Briefverkehr, an einem Empfangsschalter etc.) aber darf es nicht erforderlich sein, dass jeweils explizit die Information – sei es bspw. mit einem Hinweis auf die betriebliche Datenschutzerklärung – erfolgen muss. In diesen Fällen ist es zumutbar, dass der oder die Betroffene die Unternehmenswebseite konsultiert, um sich dahingehend zu informieren. Dies muss im erläuternden Bericht klargestellt werden; über eine Website kann i.S. der Informationspflicht nach Art. 19 Abs. 1 revDSG wirksam informiert werden, zumindest wenn die Website klar dem Verantwortlichen zuordenbar und die Information auf der Website leicht aufzufinden ist.

➔ **Art. 15 E-VDSG – Information bei der Bekanntgabe von Personendaten**

Diese sehr einschneidende Informationspflicht hat keine Grundlage im revDSG und stellt ein zusätzliches «Swiss Finish» dar. Zudem soll gemäss Entwurf nebst dem Verantwortlichen auch der Auftragsbearbeiter oder die Auftragsbearbeiterin verpflichtet werden. Dabei wird ausser Acht gelassen, dass diesem oder dieser die geforderten Angaben – zu deren Bekanntgabe er oder sie gemäss dieser Bestimmung verpflichtet wäre – idR. gar nicht vorliegen. Die Bestimmung wurde gemäss erläuterndem Bericht an Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680 angepasst; weshalb aber die Pflicht auch für private Datenbearbeitende gelten solle, wird nicht ausgeführt. Die europäische Regelung spricht unmissverständlich von den «zuständigen Behörden» weshalb die Ausweitung auf Private klar abgelehnt wird.

Empfehlung: Streichung von Art. 15 E-VDSG

➔ **Art. 16 E-VDSG – Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten**

Diese zusätzliche Pflicht für die Verantwortlichen wurde bereits im Vorentwurf des revDSG vorgeschlagen und verworfen. Entsprechend besteht keine Grundlage und sie darf keinen Einzug in die E-VDSG finden. Umso mehr, als dass die Pflicht um «die Einschränkung der Bearbeitung» erweitert wurde. Damit würde ein der revDSG fremdes Betroffenenrecht Einzug in die Verordnung finden. Es ist nicht akzeptabel, dass versucht wird bereits verworfene Bestimmungen durch die Hintertüre auf Verordnungsebene (wider-)einzuführen.

Empfehlung: Streichung von Art. 16 E-VDSG

➔ **Art. 18 E-VDSG – Form und Aufbewahrung der Datenschutz-Folgenabschätzung**

Der Text dieser Bestimmung ist dahingehend zu präzisieren, dass nebst der «schriftlichen» Form auch andere Formen, welche einen «Nachweis durch Text» ermöglichen (bspw. E-Mail), zulässig sein müssen.

Die Aufbewahrungspflicht von zwei Jahren fand kein Einzug im revDSG und wurde im Rahmen des Vernehmlassungsverfahrens bereits verworfen. Mangels gesetzlicher Grundlage ist diese ebenfalls aus der Verordnung zu streichen.

Empfehlung: Art. 18 Abs. 1 E-VDSG: *«Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in einer anderen Form, die den Nachweis durch Text ermöglicht, festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~»*

HotellerieSuisse

3. Über HotellerieSuisse

HotellerieSuisse ist das Kompetenzzentrum für die Schweizer Beherbergungsbranche und vertritt als Unternehmerverband die Interessen der innovativen und nachhaltigen Beherbergungsbetriebe der Schweiz. Seit 1882 steht HotellerieSuisse gemeinsam mit über 3'000 Mitgliedern, davon über 2'000 Hotelbetriebe, für eine qualitätsbewusste und vorausschauende Schweizer Beherbergungswirtschaft. Als Leitbranche des Tourismus beschäftigt die Beherbergung über 75'000 Mitarbeitende und stellt mit 4,5 Milliarden Franken oder 23 Prozent den zweitgrössten Anteil an der touristischen Bruttowertschöpfung dar. Im Jahr 2019 erzielte der Tourismus mit einer Nachfrage von 47 Mrd. Franken eine direkte Bruttowertschöpfung von ca. 19,5 Mrd. Franken – was einem Anteil von 2,8 Prozent an der gesamtwirtschaftlichen direkten Bruttowertschöpfung der Schweiz entspricht. Der Tourismus gehört zudem zu den fünf wichtigsten Exportbranchen und stellt mehr als 5 Prozent der gesamten Exporteinnahmen der Schweiz dar. Die Mitgliederbetriebe von HotellerieSuisse verfügen über zwei Drittel des Schweizer Bettenangebotes und generieren damit rund drei Viertel der entsprechenden Logiernächte. Als Dachverband von 13 regionalen Verbänden ist HotellerieSuisse in allen Landesteilen und Sprachregionen präsent und beschäftigt rund 100 Mitarbeitende.

Wir danken für die Kenntnisnahme unserer Position und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
HotellerieSuisse

Claude Meier
Direktor

Nicole Brändle Schlegel
Leiterin Arbeit, Bildung, Politik

HotellerieSuisse, Monbijoustrasse 130, Postfach, CH-3001 Bern
T +41 31 370 41 11, welcome@hotelleriesuisse.ch, www.hotelleriesuisse.ch

IGEM Interessengemeinschaft elektronische Medien, Wildbachstr. 3, 8008 Zürich

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

per E-Mail an jonas.amstutz@bj.admin.ch eingereicht

Zürich, 13. Oktober 2021

Stellungnahme zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, an der Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) teilnehmen zu können.

Die Interessengemeinschaft Elektronische Medien (IGEM) ist ein schweizerischer Verein, der sich seit 1998 für die Vielfalt und Transparenz der elektronischen Medien und des Internets einsetzt.

Die IGEM vereinigt die Anbieter und Abnehmer von Werbezeiten in elektronischen Medien und im Internet. Mitglieder der IGEM sind TV- und Radio-Veranstalter, Verlagshäuser und Medienunternehmen, Mediaagenturen und Vermarktungsfirmen von Werbung in TV, Radio, Kino, Teletext, digitaler Aussenwerbung und Internet, aber auch die für die Branche wichtigen Marktforschungsunternehmen und die Telekommunikationsfirmen.

Die IGEM befasst sich intensiv mit der Digitalisierung der elektronischen Medien und setzt sich insbesondere für liberale gesetzliche Rahmenbedingungen und vielfältige Möglichkeiten der kommerziellen Kommunikation in diesen Medien ein.

Wir erlauben uns deshalb, Ihnen im Folgenden unsere Stellungnahme zukommen zu lassen.

Wir danken Ihnen für die Kenntnisnahme und stehen für Fragen und Diskussionen gerne zur Verfügung.

Freundliche Grüsse

IGEM

Stephan Küng
Präsident

Siri Fischer
Geschäftsführerin

Vernehmlassung zum Entwurf der Verordnung zum revidierten DSG vom 23. Juni 2021

Streichungs- und Anpassungsvorschläge

Vorbemerkungen:

- Zahlreichen Bestimmungen fehlt eine gesetzliche Grundlage[1] oder sie widersprechen gar direkt dem Willen des Gesetzgebers (insbesondere, was die an zahlreichen Stellen neu eingeführten Dokumentationspflichten betrifft). Sie sind daher zu streichen. Das gilt insbesondere im Bereich der Datensicherheit, deren Verletzung zu einer Strafbarkeit führen soll. Die Voraussetzungen hierfür sind in diesen Fällen jedoch nicht erfüllt, weshalb die Bestimmungen ins Leere schiessen.
- Die Verordnung sollte auf zu detaillierte Bestimmungen verzichten. Die Vielfalt der Bearbeitungsaktivitäten und Situationen ist so gross, dass Details in aller Regel mehr unbeabsichtigte negative Folgen haben als für Rechtssicherheit zu sorgen. Regelungen nach dem Giesskannenprinzip machen im Datenschutz schlicht keinen Sinn, sondern sind kontraproduktiv.
- Es sollten noch Übergangsfristen von 1 Jahr ab Inkrafttreten des revDSG für die Erstellung der Verzeichnisse und – falls darauf entgegen den Anträgen nicht verzichtet wird – auch für das Bearbeitungsreglement vorgesehen werden.
- Es wäre sinnvoll, bei den einzelnen Verordnungsbestimmungen jeweils auf den Artikel der revDSG verwiesen werden, um dessen Konkretisierung es geht.

[1] «Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus (Art. 164 Abs. 2 BV). Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen (Art. 182 Abs. 2 BV). Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die **Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck.**» (BGE 141 II 169, E. 3.3).

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
1 Abs. 1	Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a. Zweck, Art, Umfang und Umstände der Datenbearbeitung; b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen; c. der Stand der Technik; d. Implementierungskosten.	Zu Abs. 1: Massnahmen zur Datensicherheit sind nicht «angemessen», sondern «geeignet», wie dies Art. 8 Abs. 1 revDSG auch sagt. «Angemessen» kann nur das resultierende Sicherheitsniveau sein. Man sollte deshalb auch in Art. 1 Abs. 1 von «geeigneten» Massnahmen sprechen, um terminologische Widersprüche zu vermeiden. Problematisch ist ferner, dass der Bundesrat von der falschen Vorstellung ausgeht, dass Art. 8 revDSG, der hier konkretisiert wird, mehr als die Datensicherheit i.e.S. regelt (CIA = Confidentiality, Integrity, Availability). Es geht weder um Bearbeitungsgrundsätze noch Betroffenenrechte. Die Beispiele in den Erläuterungen sind teilweise falsch. Ob z.B. eine Bearbeitung durch eine KI oder einen Menschen erfolgt, ist für die Frage der Datensicherheit nicht relevant. Ferner ist der Begriff des «Risikos» (Bst. b) falsch formuliert. Zudem geht es hier nicht um das Bruttorisiko, sondern das Nettorisiko. Der Begriff «Implementierungskosten» impliziert, dass anderer Aufwand nicht relevant ist. Das ist falsch. Ebenso falsch ist die Ausführung in der Erläuterung, dass übermässige Kosten nicht relevant sind. Erforderlich sind nur angemessene Massnahmen, und die Angemessenheit bestimmt sich selbst nach dem Vorschlag auch nach den Kosten.	Private Bundesorgane	Statt von «angemessenen» Massnahmen ist von «geeigneten» Massnahmen zu sprechen. Zu schreiben ist: «b. die verbleibenden potenziellen Auswirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit (Restrisiko).» «Implementierungskosten» ist durch «Implementierungsaufwand» zu ersetzen.
1 Abs. 2	Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.	Der Fokus auf die «angemessenen Abstände» ist zu eng. Wesentlich ist, dass sie in «angemessener Weise» überprüft werden. Der Begriff des «Abstands» impliziert nach wie vor eine Periodizität, die aber nicht zwingend ist, etwa wenn sich die Umstände nicht verändert haben.	Private Bundesorgane	Statt «angemessenen Abständen» ist «angemessener Weise» zu schreiben.
2	Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen: a. Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen.	Die Verwendung des Worts «erreichen» impliziert, dass die Schutzziele vollständig erfüllt werden, was weder erforderlich noch möglich ist. Zu treffen sind nur angemessene Massnahmen; eine vollständige Sicherheit ist nicht erforderlich. Die aufgeführte Liste ist überdies veraltet, zu absolut und zu detailliert formuliert. Zudem geht es grundsätzlich um die	Private Bundesorgane	Statt «erreichen» ist «anstreben» zu schreiben. Der Katalog der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	b. Zugangskontrolle: Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt. c. Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht. d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert. e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert. f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden. h. Bekanntgabekontrolle: Es kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden. i. Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden. j. Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität). k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.	Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. So ist es auch in Art. 32 Abs. 1 lit. b DSGVO definiert. Die Regelung zwingt zu einer Dokumentation für jede Datenbearbeitung (u.a. warum bestimmte der aufgeführten Schutzziele nicht relevant sind im konkreten Fall). Das widerspricht dem Willen des Gesetzgebers, der eine solche umfassende Dokumentationspflicht abgelehnt hat.		In diesem Fall wäre die Liste auch konform mit Art. 32 DSGVO.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
3 Abs. 1	Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.	Diese Bestimmung ist in mehrerlei Hinsicht problematisch und sollte ersatzlos gestrichen werden: *Erstens* fehlt ihr eine gesetzliche Grundlage. Es geht hier nicht primär um die Protokollierung zur Gewährleistung der Datensicherheit, sondern sie dient in erster Linie der *nachträglichen* Feststellung, ob es zu einer unbefugten Bearbeitung des Verantwortlichen bzw. seines Auftragsbearbeiters gekommen ist. Sollen unerlaubte Datenabflüsse, Malware, Einbrüche etc. entdeckt werden, sind andere Dinge zu protokollieren als die reguläre Nutzung der Daten (die Hacker und Malware vermeiden oder löschen werden). Zur Feststellung einer Verletzung der Datensicherheit eignet sie also nicht und ist damit unverhältnismässig. Art. 8 revDSG, welcher als Grundlage der Bestimmung dient, behandelt nur die Datensicherheit i.e.S. Nur solche sollte der Bundesrat gemäss Art. 8 Abs. 3 revDSG ausführen (und nur die Verletzung solcher können auch zu einer Strafbarkeit führen). *Zweitens* ist das Ergebnis der DSFA kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. In der Regel wird eine DSFA nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenbearbeitung. Dies hat jedoch mit Datensicherheit nichts zu tun. Die Erläuterungen des E-VDSG bestätigen sogar, dass es (auch) um die Gewährleistung der zweckkonformen Bearbeitung geht. *Drittens* muss eine solche Bearbeitung kraft Art. 21 revDSG ohnehin dem EDÖB oder Datenschutzberater vorgelegt werden. Eben dies dient bereits dem Ziel, eine solche oder andere Massnahme vorzuschlagen, soweit die Bearbeitung überhaupt umgesetzt werden kann. Hier pauschal eine spezifische Massnahme ohne Berücksichtigung der Umstände vorzuschlage ist ein Schuss ins Blaue. *Viertens* obliegt die Pflicht auch dem Auftragsbearbeiter, der jedoch die DSFA nicht kennen muss und eine solche schon gar nicht auszuführen hat. Massnahmen zur Datensicherheit obliegen zwar auch ihm, aber diese Protokollierung ist in ihrem Kern keine solche. Das erklärt den unlösbaren Widerspruch. Auch deshalb ist sie zu streichen. Unklar ist aufgrund der Norm, ob eine Protokollierungspflicht auch dann bestehen soll, wenn eine Datenschutz-Folgenabschätzung unterlassen wurde, obwohl sie nötig gewesen wäre. Dies wird aber wohl so sein.	Private	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung erreicht das Ziel materiell nicht und zielt an der Sache vorbei.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
3 Abs. 2	Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.	Die Pflicht zur Protokollierung besteht unabhängig vom Risiko und muss daher bei jeder automatisierten Bearbeitung von Personendaten vorgenommen werden. Der Begriff der automatisierten Bearbeitung ist nicht definiert. Zu verstehen ist darunter aber das Gegenteil zur manuellen Bearbeitung – somit ist darunter eine elektronische oder vergleichbare Datenbearbeitung zu verstehen. Die Protokollierungen erscheinen als unverhältnismässig – insbesondere, da auch das Lesen protokolliert werden muss. Auch im Falle von Bundesorganen ist die Regelung systematisch falsch und ohne gesetzliche Grundlage. Vgl. dazu die obigen Ausführungen.	Bundesorgan	Streichen (vgl. oben)
3 Abs. 3	Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.	Widerspruch zu den Mindestanforderungen an die Protokollierung gemäss den Absätzen 1 und 2. Abs. 3 bringt allerdings ebenfalls zum Ausdruck, dass es nicht um Verletzungen der Datensicherheit, sondern um etwaige unzulässige Bearbeitungen durch reguläre Benutzer geht. Diese stellen keine solche Verletzungen dar. Mit Empfänger ist die Organisation, nicht die Einzelperson gemeint.	Private Bundesorgane	Streichen (vgl. oben)

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
3 Abs. 4	Die Protokolle sind während zwei Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.	Für eine solche Aufbewahrungspflicht gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet, abgesehen vom Verzeichnis. Die Regelung der getrennten Aufbewahrung ist technisch nicht ohne Weiteres oder nur mit erheblichem Aufwand umsetzbar. Protokolle werden dort erzeugt, wo sie anfallen – und nicht auf anderen Systemen. Ein Betrieb müsste somit von sämtlichen Protokollen Kopien anfertigen und sie manuell auf ein anderes System übertragen; der Aufbewahrungsort muss ein unabhängiges System sein. Dieser Vorgang birgt seinerseits Sicherheitsrisiken, abgesehen davon, dass der Aufwand enorm wäre Es würde genügen, wenn sichergestellt wird, dass die Protokolle ihrerseits sicher sind. Die Personen, welche die Verletzung von Datenschutzvorschriften verfolgen, erhalten gemäss Wortlaut keinen Zugang zu den Daten. Die Zweckbindung ist unzulässig, da sie strenger ist, als die Bearbeitungsgrundsätze dies erlauben. Damit fehlt der Regelung eine gesetzliche Grundlage. Ein Verantwortlicher oder Auftragsbearbeiter hat möglicherweise ein Interesse, die Logs auch aus anderen Gründen auszuwerten. Tut er dies DSG konform, sollte dies auch möglich sein. Die Regelung ist insofern interessant, als heute viele Protokolle von IT-Systemen aus Gründen des Datenschutzes weniger lang aufbewahrt werden. Es kann mit Verweis auf den E-VDSG vertreten werden, dass eine Aufbewahrung von zwei Jahren ohne Weiteres verhältnismässig ist, wenn sogar der Gesetzgeber diese Frist standardmässig vorschreiben will. Korrekterweise ist die Aufbewahrungsfrist aber als Mindestfrist auszugestalten. Gibt es Gründe, sie länger aufzubewahren, muss dies möglich sein.	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. «getrennt vom System, in welchem die Personendaten bearbeitet werden» ist zu streichen und durch «sicher» zu ersetzen. Die Regelung ist unverhältnismässig. Sofern eine Aufbewahrungsfrist überhaupt festgelegt wird, wofür es keine Grundlage gibt, so macht eine starre Frist keinen Sinn und wäre unverhältnismässig. Sie muss von der Dauer der Datenbearbeitung abhängig und generell angemessen sein. Satz 2 ist zu streichen, da er dem DSG widerspricht, indem er die Bearbeitungsgrundsätze aushebelt. Ohnehin müsste der Personenkreis mit Zugang ist um jene erweitert werden, welche die Verletzung von Datenschutzvorschriften verfolgen.
4 Abs. 1	Bearbeitungsreglement von privaten Personen 1 Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie:	Die Pflicht, für Datenbearbeitungen mit einem hohen Risiko Bearbeitungsreglemente zu erstellen, besteht bereits nach der geltenden Verordnung. Allerdings wurde allgemein erwartet, auch aufgrund der Botschaft des Bundesrats und der parlamentarischen Beratung, dass die Bearbeitungsreglemente angesichts der neu eingeführten Dokumentations- und Informationspflichten (Verzeichnisse von Bearbeitungstätigkeiten, Datenschutz-Folgenabschätzungen, Datenschutzerklärungen) aus der Verordnung gestrichen werden.	Private	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung ist unverhältnismässig und redundant. Es ist ein Swiss Finish.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen.	Demgegenüber steht der enorme Aufwand, den die Erstellung und Nachführung eines solchen Bearbeitungsreglements mit sich bringt. Wie bei Abs. 2 gezeigt wird, werden die wesentlichen Angaben ohnehin bereits im Rahmen der in solchen Fällen erforderlichen Datenschutz-Folgenabschätzung dokumentiert, der Rest im ohnehin zu erstellenden Inventar. Die Regelung ist somit überflüssig. Auch die DSGVO sieht eine solche Regelung nicht vor (Swiss Finish). Während ein «Profiling mit hohem Risiko» in der Praxis vermutlich kaum vorkommen wird, stellt sich die Frage, ab wann «umfangreich» besonders schützenswerte Personendaten bearbeitet werden. Dies dürfte mit Bezug auf die HR-Daten bei einem mittleren und grösseren Umfang bereits der Fall sein. Auch jedes Medienunternehmen wird erfasst sein, welches Berichte über Politik und Gesellschaft enthält und damit auch besonders schützenswerte Personendaten (politische Ansichten etc.) bearbeitet. Es ist klar, dass besonders heikle Datenbearbeitungen eine betriebsinterne Regelung erfordern können. Dieser Aspekt ist jedoch über Art. 7 Abs. 1 revDSG bereits hinreichend geregelt. Der Erläuterungsbericht suggeriert, dass das Bearbeitungsreglement ein in sich geschlossenes Dokument sein muss. Dies ist praxisfremd und unnötig. Eine solche Pflicht zur «Urkundeneinheit» gilt auch sonst nirgends. Es besteht ferner das Risiko, dass Auskunftsersuchende über die Generalklausel versuchen werden, an das Bearbeitungsreglement heranzukommen. Die Dokumentationspflichten wurden aus der DSGVO übernommen und zusätzlich soll diese bestehende Pflicht nicht gestrichen werden. Dies führt zu einer erheblichen Erweiterung der Dokumentationspflichten.		

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
4 Abs. 2	Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. zur internen Organisation; e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; k. j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.	Lit. a, b, c und f sind auch Bestandteile der Bearbeitungsverzeichnisse. Die übrigen Punkte müssen bei einer Datenschutz-Folgenabschätzung mitberücksichtigt werden, wenn diese für die Risikoabwägung bzw. als Massnahme zur Reduktion der Risiken relevant sind, was in der Regel der Fall sein wird. Somit sind sie bereits dokumentiert. Die Liste zeigt im Übrigen, dass es augenscheinlich primär nicht um Datensicherheit, sondern die Einhaltung der Bearbeitungsgrundsätze und des restlichen Datenschutzgesetzes geht.	Private	Streichen (vgl. oben)

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
4 Abs. 3	Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.	Damit wird eine Pflicht zur Vorlage an den Datenschutzberater / die Datenschutzberaterin festgelegt, obwohl keine gesetzliche Verpflichtung besteht, diese Funktion überhaupt zu besetzen. Das Bearbeitungsreglement des Privaten muss weder publiziert noch dem EDÖB gemeldet werden.	Private	Streichen (vgl. oben). In jedem Fall den zweiten Halbsatz streichen.
5 Abs. 1	Das verantwortliche Bundesorgan und dessen Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie: a. besonders schützenswerte Personendaten bearbeiten; b. ein Profiling durchführen; c. Datenbearbeitungen im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG ausführen; d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen werden Personendaten zugänglich machen; e. Datenbestände miteinander verknüpfen; oder f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.	Aufgrund der Auflistung muss praktisch für jede automatisierte Bearbeitung ein Reglement erstellt werden. Es ist unklar, warum die Bearbeitungsreglemente trotz Einführung der Verzeichnisse und der Datenschutz-Folgenabschätzung beibehalten werden. Zudem fehlt aus den zu Art. 4 E-VDSG erwähnten Gründen eine gesetzliche Grundlage. Vgl. im Übrigen die obigen Ausführungen zu Art. 4 E-VDSG.	Bundesorgane	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung ist unverhältnismässig.
5 Abs. 2	Das Reglement muss mindestens die Angaben nach Artikel 4 Absatz 2 enthalten.	Die Formulierung ist unklar: Soll sie bedeuten, dass es allenfalls mehr Angaben enthalten muss?	Bundesorgane	Streichen (vgl. oben)

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
5 Abs. 3	Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen	Pflicht, das Bearbeitungsreglement dem Datenschutzberater und dem EDÖB bereitzustellen (auf Anfrage).	Bundesorgane	Streichen (vgl. oben)
6 Abs. 1	Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.	Der erste Satz wiederholt einerseits eine Banalität, ist andererseits aber ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall eingeschränkt ist, auch dann, wenn ihm nichts vorgeworfen werden kann. Dem ist nicht so. Es ist ohnehin nicht klar, was «für den Datenschutz verantwortlich» meint. Strafrechtliche Verantwortlichkeit kann es nicht sein, und aufsichtsrechtliche Verantwortlichkeit setzt ebenfalls Kontrollmöglichkeiten voraus. Wird die Verantwortlichkeit schliesslich als zivilrechtliche Haftung verstanden, dann wird mit dieser Regelung eine vom Gesetzgeber nicht vorgesehene Kausalhaftung eingeführt. Hierfür fehlt eine gesetzliche Grundlage. Dies würde auch über Art. 82 Abs. 3 DSGVO hinausgehen. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR. Die Formulierung «sicherstellen» ist zudem inhaltlich falsch. Der Verantwortliche kann nur «dafür Sorge tragen». Auch der zweite Satz ist mangelhaft, da ihm ebenfalls eine gesetzliche Grundlage fehlt. Nach Art. 9 Abs. 1 Bst. a revDSG hat der Verantwortliche zu sorgen, dass die Daten so bearbeitet werden, wie er es selbst darf. Nach Satz 2 hat er jedoch auch für die Durchsetzung seines eigenen Vertrags zu sorgen, selbst wenn dieser strenger sein sollte als das Gesetz. Macht er also einen zu strengen Vertrag, aber erlaubt er seinem Auftragsbearbeiter eine Bearbeitung, die noch dem Gesetz entspricht, ist diese Vorschrift bereits verletzt. Gemeint ist vielleicht auch eine Bezugnahme auf Art. 9 Abs. 1 DSG («… Bearbeitung … kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden…). Dies müsste in der Verordnung aber auch nicht wiederholt werden. Die Regel verwirrt also mehr als sie nutzt. Schon nach Art. 9 Abs. 1 Bst. a revDSG hat der Verantwortliche dafür zu sorgen, dass das DSG eingehalten wird. Das genügt.	Private Bundesorgane	Satz 1 streichen, da kein Mehrwert, jedoch verwirrend und falls als Kausalhaftung verstanden ohne gesetzliche Grundlage. Ohnehin ist «sicherstellen» durch «dafür Sorge tragen» zu ersetzen. Satz 2 streichen, da kein Mehrwert, jedoch verwirrend und ohne gesetzliche Grundlage, was die Pflicht zur Vertragsdurchsetzung betrifft.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
6 Abs. 2	Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.	Der Sinn und Zweck dieser Regelung erschliesst sich nicht, da der Regelungsgehalt bereits durch die Art. 16 und 17 revDSG (Bekanntgabe von Personendaten ins Ausland) gedeckt ist. Gemäss Erläuterungsbericht entspricht der neue Art. 6 Abs. 2 E-VDSG dem geltenden Art. 22 Abs. 3 VDSG. Dabei handelt es sich aber um eine Bestimmung für Bundesorgane, während Art. 6 Abs. 2 E-VDSG sowohl für Datenbearbeitungen Privater als auch für solche von Bundesorganen gelten soll. Aus dem Erläuterungsbericht geht nicht hervor, warum diese Bestimmung nun auch für Private gelten soll (oder warum es sie überhaupt braucht bzw. auf welche Rechtsgrundlage sie sich stützt). Die Regelung würde nur dort halbwegs Sinn machen, wo ein Schweizer Verantwortlicher einen ausländischen Auftragsbearbeiter bemüht Daten zu bearbeiten, ohne dass es zu einer Bekanntgabe aus der Schweiz kommt und somit Art. 16 revDSG nicht greift. Systematisch wäre aber auch dieser Fall in Art. 16 revDSG zu regeln und nicht in der VDSG. Es ist dies ein absoluter Sonderfall. Eine eigene Regelung in der VDSG rechtfechtfertigt sich dadurch nicht. Die Regelung ergibt sich im Übrigen sowieso bereits aus Art. 9 Abs. 1 Bst. a revDSG, und zwar systematisch korrekt, während sie hier systematisch falsch angelegt ist: Im Falle einer Auftragsbearbeitung geht es um die Sicherstellung eines gleichwertigen Datenschutzes, da der Auftragsbearbeiter die Daten gar nicht in eigener Regie bearbeiten darf. Es geht darum sicherzustellen, dass die Daten nur so bearbeitet werden, wie der Verantwortliche dies darf – und so steht es schon in Art. 9 Abs. 1 Bst. a revDSG. Es ist allerdings zweifelhaft, ob die Autoren der Regelung diesen Sonderfall überhaupt im Blick hatten. Vermutlich wurde die Regel einfach übernommen, weil es sie schon gab.	Private Bundesorgane	Streichen. Die Regelung steht im Konflikt mit Art. 16 f. revDSG und Art. 9 Abs. 1 Bst. a revDSG, welche diesen Sachverhalt bereits abschliessend regeln.
6 Abs. 3	Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter	Gemäss den Erläuterungen zum E-VDSG schliesst die schriftliche Form auch die elektronische Form mit ein. Damit entspricht die Formulierung von Art. 28 Abs. 2 DSGVO, welche	Bundesorgane	Klarstellung, dass eine Genehmigung in Textform genügt und sie auch in allgemeiner Form

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich genehmigt hat.	ebenfalls «schriftlich» vorschreibt, damit aber auch den Fall des Nachweises durch Text meint. Es sollte ferner klargestellt werden, dass eine allgemeine Genehmigung (analog zur Regelung der DSGVO) zulässig ist, da es Bundesorganen sonst nicht möglich sein wird, Dienste von Standard-Online-Services zu beziehen. Diese verwenden ausschliesslich diese Methode.		erfolgen kann (beides analog DSGVO).
7	Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften entstehen.	Die Formulierung der Norm ist zu salopp. Es ist nicht klar, was «Probleme» sind. Die Norm stellt aber klar, dass Art. 28 Abs. 2 lit. a E-VDSG die Datenschutzberater*in *nicht* verpflichtet ist, *jede* Datenbearbeitung zu prüfen; andernfalls wäre eine Information bei Auftragsbearbeitungsverträgen a priori nicht erforderlich.	Bundesorgane	Satz 2 ist zu streichen, da unnötig. Jedenfalls ist er präziser zu formulieren.
9 Abs. 1	Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen mindestens die folgenden Punkte regeln: a. die Anwendung der Grundsätze der Recht-mässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung und der Richtigkeit; b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen; c. die Art und der Zweck der Bekanntgabe von Personendaten; d. die Namen der Staaten, in die Personendaten bekanntgegeben werden; e. die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden; f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;	Die Aufzählung der Anforderungen an einen «Data Transfer Agreement» ist untauglich, weil sie nicht zwischen der Art der Übermittlung bzw. Rollen des Exporteurs und Importeurs unterscheidet. Diese sind jedoch für den Inhalt des Vertrags entscheidend, wie beispielsweise die vom EDÖB inzwischen anerkannten Standardvertragsklauseln der Europäischen Kommission (EU SCC) zeigen. So macht es keinen Sinn, einen Auftragsbearbeiter im Ausland zur Anwendung der Bearbeitungsgrundsätze, zur Information der betroffenen Personen oder zur Wahrung der Rechte der betroffenen Personen zu verpflichten. Sie müssten dem auch nach revDSG nicht nachkommen, weshalb nicht einzusehen ist, dass sie hierzu vertraglich verpflichtet werden sollen. In den Bearbeitungsgrundsätzen (Bst. a) fehlt der Grundsatz der Transparenz. Keine rechtliche Grundlage hat das Erfordernis in Bst. d und e, den Namen der Staaten oder der internationalen Organisationen zu nennen, denen Personendaten bekanntgegeben werden, soweit hiermit Weiterübermittlungen gemeint sind, was	Private Bundesorgane	Der Anforderungskatalog kann gestrichen werden, da der EDÖB sie sowieso prüfen muss. Wird dies nicht getan, ist der Anforderungskatalog entweder anzupassen, um unterschiedliche Konstellationen abzudecken (Controller, Processor) oder das «mindestens» ist durch «je nach den Umständen» zu ersetzen. Bst. a ist um den Grundsatz der Transparenz zu erweitern. Bst. d, e und f sind zu streichen.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger; h. die Massnahmen zur Gewährleistung der Datensicherheit; i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ; j. die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren; k. die Rechte der betroffenen Person, namentlich: 1. das Auskunftsrecht, 2. das Widerspruchsrecht, 3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten, 4. das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen.	nicht klar ist. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Auch die EU SCC beschränken sich darauf. Bst. f ist bereits mit dem Grundsatz der Verhältnismässigkeit abgedeckt und damit redundant. Bst. g geht zu weit, indem es die «berechtigten» Empfänger verlangt. Relevant sind die «Empfänger», also normalerweise die Parteien, welche den Vertrag abschliessen und damit bereits ersichtlich sind. Es fehlen Regelungen zur Meldung von Verletzungen der Datensicherheit, insbesondere soweit die betroffenen Personen zu informieren sind.		Meldungen betr. eine Verletzung der Datensicherheit sind zu regeln.
9 Abs. 2	Der Verantwortliche muss angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.	Der Begriff "sicherzustellen" impliziert eine Garantie der Einhaltung der Klauseln bzw. Kausalhaftung, wofür es keine gesetzliche Grundlage gibt und die vernünftigerweise auch nicht verlangt werden kann.	Private Bundesorgane	Der Begriff «sicherstellen» ist durch «in angemessener Weise Sorge zu tragen» zu ersetzen.
10 Abs. 1	Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.	Massnahmen sind angemessen, wenn sie dem Stand der Technik sowie den konkreten Umständen entsprechen. Die Anforderungen an die Massnahmen sind höher, wenn es sich beispielsweise um besonders schützenswerte Personendaten handelt. Wiederum kann der Exporteur nicht «sicherstellen», sondern nur dafür Sorge tragen. Der Erläuterungsbericht verlangt fälschlicherweise, dass der Empfänger verpflichtet werden muss, das Schweizer Datenschutzrecht einzuhalten. Das ist falsch. Einhalten muss er nur den Vertrag.	Private Bundesorgane	Der Begriff «sicherstellen» ist durch «in angemessener Weise Sorge zu tragen» zu ersetzen.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Die Vorschrift führt zu einer Kausalhaftung und ist in der Praxis nicht zu erfüllen. Nicht einmal das Bankenrecht kennt eine derart strenge Regelung. Zudem verlangen die aktuellen Standardvertragsklauseln, die in der Praxis flächendeckend eingesetzt werden, ohnehin entsprechende Sorgfaltspflichten des Exporteurs.		
12 Abs. 2	Der Verhaltenskodex enthält mindestens die Angaben nach Artikel 9 Absatz 1 und muss vorgängig vom EDÖB genehmigt werden.	Dies wird nicht möglich sein, da der Verhaltenskodex naturgemäss abstrakt und nicht für spezifische Unternehmen formuliert ist. Er wird somit beispielsweise die «Empfänger» (nicht: «Kategorien von Empfängern») nicht nennen. Dies ist jedoch gemäss dieser Bestimmung erforderlich. Ferner sollte nicht von «Angaben» die Rede sein, sondern von «Regelungen» oder «Punkten».	Private Bundesorgane	Der Verhaltenskodex «muss mindestens jene Punkte regeln, die nach dem Sinn und Zweck von Art. 9 Absatz 1 zu Regeln sind.»
13 Abs. 1	Der Verantwortliche und der Auftragsbearbeiter teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit.	Art. 13 Abs. 1 E-VDSG verweist auf eine Informationspflicht des Auftragsbearbeiters, was im Erläuterungsbericht auch nochmals ausdrücklich betont wird. Das revDSG sieht aber keine Informationspflicht des Auftragsbearbeiters vor, diese besteht gemäss Art. 19 revDSG (korrekterweise) nur für den Verantwortlichen. Da das Gesetz keine solche Pflicht für den Auftragsbearbeiter vorsieht, kann sie auch nicht über die Verordnung eingeführt werden. Art. 19 revDSG verlangt eine Information der betroffenen Personen, nicht eine Mitteilung. Für eine Information der betroffenen Person genügt ein Zugänglichmachen. Dies entspricht auch dem Verständnis unter der DSGVO. Es sollte durch die Wortwahl «mitteilen» keine Verschärfung impliziert werden. Stattdessen sollte analog zu den Informationspflichten im Finanzmarktrecht der Begriff «zur Verfügung stellen» verwendet werden. Das bringt auch besser zum Ausdruck, dass die Information ein Betroffenenrecht darstellt, dessen Ausübung eine gewisse Mitwirkung des Betroffenen verlangt. Die Erläuterungen erwähnen, dass eine Kommunikation über eine Website nicht immer genügt. Die Person müsse wissen, dass sie die Informationen auf einer bestimmten Website findet, und es wird z.B. für Telefongespräche nahegelegt, dass ihr der Link mündlich mitgeteilt wird. Solche Ausführungen sind	Private Bundesorgane	Die Erwähnung des Auftragsbearbeiters ist zu streichen. Es fehlt die gesetzliche Grundlage. Seine Erwähnung macht auch keinen Sinn. Es sollte nicht das Wort «mitteilen» verwendet werden, da es dafür keine gesetzliche Grundlage gibt. Korrekt wäre «Der Verantwortliche stellt die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form zur Verfügung.» Es sollte festgehalten werden, dass eine Information über eine Website in der Regel genügt.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		praxisfremd. Es sollte stattdessen festgehalten werden, dass die Information auf der Website genügt. Das entspricht der heutigen Praxis. Alles andere ist praxisfremd. Auch die Ausführungen in den Erläuterungen, wonach die betroffene Person die wichtigsten Informationen stets auf der ersten Kommunikationsstufe erhalten muss, ist schlicht falsch. Es gibt hierfür keine gesetzliche Grundlage, und es lässt jede Selbstverantwortung ausser Acht. Das ist auch deshalb bedenklich, weil der betroffenen Personen im Datenschutz eine Schlüsselrolle zukommt und es kontraproduktiv ist, ihr jede Eigeninitiative abzunehmen.		
13 Abs. 2	Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.	Werden Piktogramme verwendet, müssen diese maschinenlesbar sein. Letzteres soll gemäss dem Erläuterungsbericht einen Vergleich verschiedener Dokumente und allgemein eine gewisse Automatisierung ermöglichen – es stellt sich die Frage, inwieweit dies ein Ziel des Datenschutzes ist. Die Pflicht unterliegt auch einem Überlegungsfehler. Die Piktogramme haben den Zweck, den Menschen einfacher als über Text anzusprechen und ihm zu ermöglichen, intuitiv auf eine Datenschutzerklärung zu reagieren. Soll dagegen eine automatisierte Auswertung einer Datenschutzerklärung erfolgen, müsste die Datenschutzerklärung selbst, nicht die Piktogramme maschinenlesbar bzw. ihre Inhalte entsprechend codiert sein, und zwar unabhängig davon, wie sie optisch dargestellt ist. Bei der Maschinelesbarkeit geht es ja gerade *nicht* um die optische Darstellung. Abgesehen davon gibt es für eine solche Pflicht keine gesetzliche Grundlage. Die Verwendung von Piktogrammen ist freiwillig, und daher darf der Verwender auch entscheiden, ob sie maschinenlesbar sind oder nicht, was auch immer dies bedeutet. Schliesslich fehlt es auch an Standards für solche Angaben. Ohne Standards macht eine solche Regel keinen Sinn.	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. Die Regel macht auch keinen Sinn und führt im schlimmsten Fall zur Strafbarkeit. Dies kann wiederum dazu führen, dass keine Piktogramme verwendet werden.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
14	Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin.	Dies betrifft insbesondere die Statistik und Forschung. Die Regelung ist jedoch praxisfremd, denn es kann auch aus den Umständen hervorgehen, dass eine Auskunft freiwillig ist (Beispiel: Kundenzufriedenheitsumfrage eines Krankenversicherers)	Bundesorgane	Ergänzen mit «soweit dies nicht aus den Umständen ersichtlich ist»
15	Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.	Für diese «Informationspflicht bei der Bekanntgabe von Personendaten» gibt es keine gesetzliche Grundlage. Sie ist auch nach EU-Recht, auf welches sich der Erläuterungsbericht beruft, für private Datenbearbeiter nicht vorgeschrieben. Gegenüber der bisherigen Regelung in der VDSG wird die Vollständigkeit neu hinzugefügt, d.h. die Daten dürfen nicht lückenhaft sein. Die Regelung ist praxisfremd. Sie lässt sich nicht vernünftig umsetzen. Soll fortan jede E-Mail an eine andere Organisation einen entsprechenden Hinweis enthalten? Dazu kommt, dass der Empfänger ohnehin selbst verpflichtet ist, die Bearbeitungsgrundsätze einzuhalten und angemessene Massnahmen zu treffen, sich über die Richtigkeit der Daten zu vergewissern. Eine Information durch die übermittelnde Person unterläuft dies bzw. verabsolutiert eine der möglichen Vergewisserungsmassnahmen. Dies widerspricht dem Gesetz. Hinzu kommt, dass ein Auftragsbearbeiter etwas bekanntgeben soll, das er womöglich gar nicht hat.	Private Bundesorgane	Streichen, jedenfalls für private Datenbearbeiter. Es gibt keine gesetzliche Grundlage. Swiss Finish. Sie ist in dieser Form nicht praktikabel.
16	Der Verantwortliche informiert die Empfängerinnen und Empfänger, denen er Personendaten bekanntgegeben hat, unverzüglich über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten, ausser die Benachrichtigung ist unmöglich oder mit einem unverhältnismässigen Aufwand verbunden.	Die in Art. 16 E-VDSG vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren, war bereits im Entwurf des revDSG vorgesehen und wurde vom Parlament gestrichen. Die Einführung dieser Pflicht über die revidierte Verordnung würde daher dem Willen des Parlaments widersprechen. Dieselbe Bestimmung verweist zudem auf ein Recht auf Einschränkung der Bearbeitung von Personendaten, das so im revDSG nicht besteht.	Private Bundesorgane	Streichen. Es gibt keine gesetzliche Grundlage.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Die Regelung erwähnt zudem die «Einschränkung» der Bearbeitung. Dies spielt auf Art. 18 DSGVO an, welche Bestimmung in der Schweiz so nicht existiert.		
18	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.	Für eine solche Aufbewahrungspflicht gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet, abgesehen vom Verzeichnis. Die Regelung geht ferner davon aus, dass eine Datenschutz Folgenabschätzung nie erneuert wird. Dies entspricht jedoch nicht der Praxis. Es ist nicht klar, wie mit mehreren Datenschutz-Folgenabschätzungen umzugehen ist.	Private / Bundesorgane	Klarstellen: «… muss in der aktuellsten Fassung während zwei Jahren …» Die Aufbewahrungspflicht ist zu streichen. Es fehlt eine gesetzliche Grundlage. So oder so ist sie als Mindestfrist auszugestalten. Es ist klarzustellen, dass Schriftlich «in Textform» meint.
19 Abs. 1	Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit: a. die Art der Verletzung; b. soweit möglich den Zeitpunkt und die Dauer; c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten; d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen; e. die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen; f. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder die Folgen zu mildern; g. den Namen und die Kontaktdaten einer Ansprechperson.	Bst. e ist falsch formuliert. Die «allfälligen Risiken» beinhalten bereits die Folgen für die betroffenen Personen. Richtig müsste es heissen «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht». Auch in Bst. f müsste nicht von den «Folgen», sondern vom «Risiko» die Rede sein. Gemildert werden kann entweder das Schadensausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem «Risiko» entspricht). Gemäss den Erläuterungen wird das in Art. 24 Abs. 2 revDSG erwähnte «voraussichtlich» so interpretiert, dass auch dann gemeldet werden muss, wenn das Vorliegen eines «hohen Risikos» nicht ausgeschlossen werden kann. Diese Aussage hilft nicht weiter, da es sich um einen Pleonasmus handelt. Der Begriff «Risiko» beinhaltet bereits eine Wahrscheinlichkeitsüberlegung, d.h. wie wahrscheinlich es ist, dass ein Schaden eintritt. Es bleibt dabei: Die Wahrscheinlichkeit muss eine gewisse Höhe aufweisen. Wünschenswert wäre schliesslich eine «de minimis»-Regelung, die jene Fälle ausschliesst, in welchen der EDÖB ohnehin nicht wirklich etwas tun kann oder will, obwohl ein hohes Risiko vorliegt (z.B. eine problematische E-Mail geht an den falschen Empfänger und ein Missbrauch durch diesen ist möglich). Damit können auch die Ressourcen des EDÖB	Private Bundesorgane	Im Einleitungssatz ist aufzunehmen: «… bei einer meldepflichtigen Verletzung …» Bst. e ist umzuformulieren: «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht» Es sollte eine «de minimis» Regelung vorgesehen werden, in welchen trotz eines hohen Risikos für eine betroffene Person nicht gemeldet werden muss. Bst. f. sollte angepasst werden: "gegebenenfalls welche Massnahmen getroffen wurden …"

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		geschont werden, die er für andere, für den Datenschutz wichtigere Angelegenheiten einsetzen kann.		
19 Abs. 2	Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.	Der Hinweis «bei Entdeckung der Verletzung der Datensicherheit» erscheint wenig sinnvoll. Zu diesem Zeitpunkt wird der Verantwortliche nie über alle Informationen verfügen, da sich diese immer erst über Zeit herausstellen. Der Hinweis kann ersatzlos gestrichen werden.		Streichung von «bei Entdeckung der Verletzung der Datensicherheit»
19 Abs. 5	Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.	Eine Dokumentationspflicht kennt zwar die DSGVO. Das revDSG sieht sie jedoch nicht vor. Daher kann sie und die entsprechende Aufbewahrungspflicht auch nicht auf dem Weg der Verordnung eingeführt werden. Noch die Botschaft zum revDSG hielt fest, dass keine allgemeine Dokumentationspflicht eingeführt werden soll. Genau dies wird hier (und in anderen Bestimmungen) durch die Hintertür versucht. Es bleibt jedenfalls unklar, wozu die Dokumentations- und Aufbewahrungspflicht dient, ausser allenfalls dem EDÖB. Da sich aus der Systematik aber ergibt, dass ohnehin nur meldepflichtige Verletzungen zu dokumentieren sind, erschliesst sich auch dieser Sinn nicht wirklich: Ist gemeldet und interessiert sich der EDÖB dafür, wird er sofort nachfragen. Tut er dies nicht, wird er kaum später darauf zurückkommen. Der Hinweis auf alle «zusammenhängenden Tatsachen» ist falsch, denn er suggeriert, dass Tatsachen nur für die Dokumentationspflicht erforscht werden müssen, was sicherlich nicht erforderlich ist. Warum hier drei statt wie sonst zwei Jahre vorgesehen sind, ist unklar.	Private Bundesorgane	Streichen. Es fehlt die gesetzliche Grundlage. Die Norm ist auch nicht nötig. Der Begriff «Tatsachen» ist durch «und dokumentierten Tatsachen» zu präzisieren.
20 Abs. 3	Die Auskunft muss für die betroffene Person verständlich sein.	Sie muss verständlich sein. Ob die betroffene Person sie im konkreten Fall versteht, ist nicht relevant. Beim Auskunftsbegehren geht es darum, die bearbeiteten Daten mitzuteilen. Müssen diese noch so erläutert werden, dass	Private Bundesorgane	Den Begriff «für die betroffene Person» streichen. Statt «verständlich» soll «im Grundsatz nachvollziehbar

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		sie für die betroffene Person verständlich sind, kann dies zu einem unverhältnismässigen Aufwand führen. Das Auskunftsrecht bietet Zugang zu Daten, nicht ein Recht darauf, die Datenbearbeitung so lange erklärt zu bekommen, bis sie die jeweilige Person versteht. Eine solche Pflicht hat keine Grundlage im Gesetz. Beispielsweise können die im Rahmen einer klinischen Studie bearbeiteten Daten oder technische Logdaten für die betroffene Person unverständlich sein. Müssen diese zuerst so dargestellt werden, dass sie für die betroffene Person verständlich sind, sind aufwändige Erläuterungen erforderlich, mitunter auch sehr viel Fachwissen. Abgesehen davon, dass dies nicht unbedingt innerhalb von 30 Tagen erfolgen kann, sprengt dies jeden Rahmen und ist unverhältnismässig. Nirgends in Europa wird das Auskunftsrecht so verstanden.		sein, sofern damit kein unverhältnismässiger Aufwand verbunden ist» verwendet werden. Eine Alternative wäre folgende Formulierung: «Die Auskunft darf nicht irreführend sein.»
20 Abs. 4	Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.	Es fehlt eine gesetzliche Grundlage für eine echte Verpflichtung der betroffenen Person. Insofern macht Satz 2 wenig Sinn. Lässt sich die Identität der betroffenen Person nicht verifizieren, erhält sie auch keine Auskunft.	Private Bundesorgane	Begriff «Identifizierung» ersetzen durch den Begriff «Authentifizierung»
20 Abs. 5	Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.	Diese Dokumentation kann bspw. durch eine Kopie des Antwortschreibens erreicht werden. Bei einer mündlichen Auskunft müsste daher z.B. eine Telefonnotiz erstellt werden. Das revDSG sieht keine solche Dokumentations- und Aufbewahrungspflicht vor. Sie kann nicht auf dem Verordnungsweg eingeführt werden. Sie ist auch wenig sinnvoll. Sie zwingt den Verantwortlichen, Personendaten entsprechend länger aufzubewahren bzw. mehr Personendaten zu beantworten, als er dies womöglich tun würde. Die betroffene Person erhält eine Antwort auf ihr Ersuchen. Will sie dagegen vorgehen, kann sie diese Antwort ins Recht legen. Die Bestimmung sorgt nur für zusätzlichen Aufwand. Wie sich die drei Jahre herleiten, ist unklar.	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. Die Bestimmung bietet keinen Mehrwert, sorgt aber für zusätzlichen Aufwand.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
21 Abs. 1	Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.	Unklar ist, welche Rechtsfolge die «Unzuständigkeit» eines Verantwortlich hat.	Private Bundesorgane	Es ist zu präzisieren: "Sind für die Bearbeitung von Personendaten mehrere gemeinsam verantwortlich …"
21 Abs. 2	Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen.	Diese Bestimmung ist verwirrlich, da sie impliziert, dass der Auftragsbearbeiter selbst eine Auskunftspflicht hat, wenn er faktisch in der Lage sein sollte, eine Auskunft zu erteilen bzw. er das Auskunftsgesuch in einem solchen Fall nicht weiterleiten muss, auch wenn er es nicht beantwortet. Das kann nicht sein. Die Regelung sollte präzisiert werden.	Private Bundesorgane	Am Ende sollte es heissen: «sofern er das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet.»
22 Abs. 1	Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen.	Die Frist kann erst dann zu laufen beginnen, wenn das Begehren klar und die betroffene Person korrekt identifiziert ist. Dies ist sie zu Beginn häufig nicht.	Private Bundesorgane	Zu präzisieren: «… seit dem Vorliegen eines klaren Begehrens und der korrekten Identifikation der betroffenen Person.»
23 Abs. 2	Die Beteiligung beträgt maximal 300 Franken.	Der Betrag wird nicht verändert, weil es seit seiner Einführung zu keiner relevanten Teuerung gekommen sei und der Betrag nicht abschreckend sein soll. Allerdings steht dieser Kostendeckel im Vergleich zum Aufwand, den ein Auskunftsersuchen trotz entsprechender Strukturen mit sich bringen kann, in keinem Verhältnis (z.B. können umfassende Schwärzungen erforderlich sein, was Kosten pro Fall von CHF 10'000 mit sich bringen kann). Auch die DSGVO kennt keine betragsmässige Begrenzung, sondern verlangt, dass er «angemessen» ist. Auch im Öffentlichkeitsrecht kann eine Gebühr verlangt werden. Der Betrag soll durchaus abschreckend sein, weil er die betroffenen Personen dahingehend diszipliniert, Auskunftsersuchen nur dann zu stellen, wenn sie wirklich angezeigt sind und nicht aus Jux.	Private Bundesorgane	Betrag den Verhältnissen anpassen (mindestens CHF 3'000) Alternativ ist die Bestimmung zu streichen, da die angemessene Kostenbeteiligung bereits in Abs. 1 enthalten ist. Beispiel: Aufwand bis CHF 500 trägt das Unternehmen, darüber hinaus müssen die Kosten zu 50% übernommen werden.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
23 Abs. 3	Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen.	Es ist zu präzisieren, dass die Antwortfrist von 30 Tagen erst danach beginnt.	Private Bundesorgane	Präzisieren: «Erst danach beginnt die Frist zur Beantwortung des Auskunftsbegehrens.»
25	Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen muss folgende Aufgaben wahrnehmen: a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden. b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.	Es ist schon konzeptionell nicht richtig, dass der Datenschutzberater die Aufgaben «wahrnehmen» muss, er muss sie «haben». Zu lit. a: Die breite der Prüfpflicht geht am Ziel vorbei, als sie impliziert, dass der Datenschutzberater im Grund kein Berater mehr ist, sondern als "Datenschutzpolizist" agieren sollte, d.h. alles und jeden in Bezug auf den Datenschutz zu überprüfen. Richtig wäre stattdessen, dass seine beratende Funktion betont wird, und zwar dort, wo ihn die verantwortlichen Stellen beiziehen wollen. Das ist auch das Prinzip, das der Gesetzgeber bei der DSFA verfolgt: Wenn der Verantwortliche die DSFA nicht dem EDÖB vorlegen will, was er kann, dann kann er sie stattdessen dem Berater vorlegen. So sieht es auch Art. 10 Abs. 2 Bst. a revDSG vor. Dem ist hier Rechnung zu tragen. Der Berater sollte nur auf Beizug aktiv werden. Abgesehen davon ist beim bestehenden Vorschlag unklar, in welchem Umfang die Bearbeitungen zu prüfen sind (alle, einige, nur die ihm vorgelegten, nur nach Risiko) und welche Folgen es hat, wenn der Datenschutzberater dieser Aufgabe nicht nachkommt. Die Erläuterungen implizieren, dass alle Bearbeitungsaktivitäten überprüft werden müssen, was nicht richtig sein kann. Auch hier kann risikoorientiert geprüft werden. Zu lit. b: Nur das Vorlegen der DSFA dem/der DSB genügt nicht, der/die DBS muss bei der Erstellung der DSFA mitwirken. Dabei müssen die Risikobewertung und vorgeschlagenen Massnahmen geprüft werden.	Private	Die Bestimmung sollte gestrichen werden, da im Gesetz bereits alles nötig gesagt wird. Sie stammt noch aus einer Zeit, in welcher das Gesetz noch keine solchen Ausführungen enthielt. Wird sie beibehalten, ist sie zu präzisieren: «Der Datenschutzberaterin oder dem Datenschutzberater eines privaten Verantwortlichen müssen folgende Aufgaben übertragen worden sein:» Bst. a ist anzupassen: "Wo sie oder er beigezogen wird, prüft sie oder er die Bearbeitung …"
26	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind	Unternehmen mit weniger als 250 Mitarbeitenden (wohl nicht FTE) müssen folglich nur diejenigen Bearbeitungstätigkeiten in Verzeichnissen dokumentieren, die die genannten Kriterien erfüllen, d.h. eine Datenbearbeitung durchführen, die ein hohes Risiko mit sich bringt.	Private	Es ist klarzustellen, dass wenn eine der beiden Voraussetzungen erfüllt ist, die Verzeichnispflicht nur für die entsprechenden Bearbeitungen mit hohem Risiko gelten.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.	Unklar ist, ab wann «umfangreich» besonders schützenswerte Personendaten bearbeitet werden. Genügt die Bearbeitung von HR-Daten? Sind die Voraussetzungen für die Befreiung nicht erfüllt, ist das Verzeichnis für alle Bearbeitungsaktivitäten zu führen. Dies impliziert jedenfalls der Wortlaut der Bestimmung. Art. 12 Abs. 5 revDSG erlaubt die Ausnahme nur, wenn ein «geringes Risiko» vorliegt. Demnach ist der Bundesrat der Auffassung, dass wenn weder Bst. a noch b erfüllt ist, per se ein geringes Risiko vorliegt. Das würde den Anwendungsbereich von Art. 22 revDSG (DSFA) stark einschränken. Zudem ist darauf hinzuweisen, dass diese Ausnahme bei Art. 3 und 4 nicht vorgesehen ist, was zu absurden Folgen führt. Generell sollten für Verzeichnisse Übergangsfristen vorgesehen werden, da sie einen sehr hohen Aufwand mit sich bringen.		Der Begriff der Mitarbeitenden ist durch "Vollzeitstellen" zu ersetzen. Es ist eine Übergangsfrist zur Umsetzung der Verzeichnispflicht von einem Jahr vorzusehen.
31	Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von Personendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden.	Es ist unklar, was «sogleich» bedeuten soll. Es muss genügen, dass die Erfordernisse des Datenschutzes im Projekt rechtzeitig berücksichtigt werden.	Bundesorgane	Der Begriff «sogleich» ist durch «rechtzeitig» zu ersetzen.
32 Abs. 1	Das verantwortliche Bundesorgan meldet dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung. Der EDÖB nimmt diese Meldung in das Register der Bearbeitungstätigkeiten auf.	Bereits geplante automatisierte Bearbeitungstätigkeiten müssen gemeldet werden, was zu einem erheblichen Mehraufwand für die Dokumentation führt. Zudem muss jede geplante automatisierte Bearbeitung gemeldet werden, nicht nur solche mit einem (potenziellen) hohen Risiko. Die Meldung muss im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung erfolgen. Diese erfolgen oft auf der Basis eines vorgegebenen Rahmens, während die konkreten Entscheidungen erst im Verlauf des Projekts getroffen	Bundesorgane	Streichen, es fehlt die gesetzliche Grundlage. Zudem liegen die zu meldenden Informationen im Zeitpunkt, in dem die Meldung erfolgen soll, in der Regel nicht in der genügenden Detailtiefe vor. Die Ressourcenplanung des EDÖB rechtfertigt zudem nicht den mit dieser frühen Meldung

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		werden. Daraus folgt, dass die verlangten Angaben in dem Zeitpunkt in der Regel noch nicht in der genügenden Detailtiefe vorliegen werden. Zudem sollte sich gemäss Botschaft zu Art. 11 Abs. 4 E-DSG (Art. 12 Abs. 4 revDSG) keine Änderung im Vergleich zum bestehenden Recht ergeben. Eine Pflicht, geplante Datensammlungen dem EDÖB zu melden, besteht aber nach geltendem Recht nicht. Es fehlt daher an einer gesetzlichen Grundlage. Gemäss Erläuterungsbericht dient die frühe Meldung zudem nicht dem Persönlichkeitsschutz, sondern der Ressourcenplanung des EDÖB. Art. 47 E-VDSG enthält eine Übergansbestimmung für automatisierte Bearbeitungstätigkeiten, die bei Inkrafttreten des EVDSG bereits produktiv sind. Diese Übergangsbestimmung ist insofern keine Erleichterung, als für bereits produktive Bearbeitungen ein Verzeichnis erstellt und dieses an den EDÖB gemeldet werden muss.		einhergehenden Mehraufwand der Bundesbehörden.

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per E-Mail an:
jonas.amstutz@bj.admin.ch

Bern, 12. Oktober 2021

Stellungnahme von INSOS Schweiz zur Vernehmlassung: Ausführungsrecht zum Datenschutzgesetz (revidierte Verordnung über den Datenschutz)

Sehr geehrte Damen und Herren

INSOS Schweiz nimmt gerne Stellung zu den Ausführungsbestimmungen zum Datenschutzgesetz. INSOS Schweiz vertritt als nationaler Branchenverband die Interessen von 800 Institutionen für Menschen mit Behinderung. 60 000 Menschen mit unterschiedlichsten Beeinträchtigungen finden dort Arbeit, eine Tagesstruktur sowie ein Zuhause und erhalten die Möglichkeit, eine Integrationsmassnahme oder eine berufliche Massnahme zu absolvieren.

Ausgangslage

Die DSG-Totalrevision umfasst zum einen die Totalrevision des DSG (E-DSG), zum andern eine Teilrevision weiterer Bundesgesetze. Das Parlament hat die Vorlage des Bundesrates in zwei Etappen aufgeteilt. In der ersten Etappe wurde nur eine EU-Richtlinie zum Datenschutz in Strafsachen (SDSG) umgesetzt und am 01.03.2019 in Kraft gesetzt. In einer zweiten Etappe hat das Parlament das neue Datenschutzgesetz (nDSG) am 25.09.2020 verabschiedet. Die vorliegende Vernehmlassung über das Umsetzungsrecht des revidierten DSG (Vorentwurf der revidierten Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)) wurde am 23.06.3021 eröffnet. Sie dauert bis am 14.10.2021.

Grundzüge der vorliegenden Stellungnahme

Da es sich im Rahmen der vorliegenden Vernehmlassung nur noch um die Gestaltung des Umsetzungsrechts einer bereits erfolgten Gesetzesrevision handelt, ist der Ermessenspielraum für Anpassungen der neuen Gesetzgebung sehr begrenzt.

Die vorliegende Vernehmlassungsantwort fokussiert auf die für die Institutionen und Strukturen für Menschen mit Unterstützungsbedarf relevanten Punkte der vom Bundesrat vorgeschlagene VDSG-Revision.

In der Stellungnahme wird in erster Linie darauf geachtet, dass die vom Bundesrat vorgeschlagenen Umsetzungsmodalitäten des revidierten Datenschutzgesetzes möglichst schlank, praxisnah und anwendungsfreundlich für die Betriebe bleiben. Das ist nicht selbstverständlich im Rahmen eines Gesetzgebungsprozesses, der nicht besonders darauf ausgerichtet ist: Dieser strebt offensichtlich vor allem eine sehr genaue und umfangreiche Einhaltung des Datenschutzes an.

Des Weiteren beantragt die vorliegende Vernehmlassungsantwort eine möglichst konkrete, zugängliche und auch finanziell günstige Unterstützung der Betriebe durch die zuständigen staatlichen Stellen – vor allem durch den Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Die in der Stellungnahme vertretenen Standpunkte berücksichtigen gleichwohl die Wichtigkeit eines zielführenden Datenschutzes: Allgemein wird davon ausgegangen, dass die Betriebe oftmals heikle Daten bearbeiten, deren Bekanntgabe ein hohes Risiko für die betroffenen Personen von Unterstützungsleistungen aufweisen können; deswegen soll an einem strikten Datenschutz nicht gerüttelt werden.

Auch wird in der vorliegenden Vernehmlassungsantwort beantragt, dass grob umrissene Begriffe und Abgrenzungen präziser umschrieben werden – dies im Sinne einer möglichst klaren Umsetzungshilfe für die betroffenen Betriebe.

Relevante Bestimmungen der E-VDSG für die ambulanten und stationären Betriebe für Personen mit Unterstützungsbedarf

E-VDSG	Kommentar	Beantragte Neuformulierung
Art. 1 Abs. 1	Die vorgeschlagene Umschreibung ist im Grundsatz zu begrüssen. Sie ergänzt und konkretisiert sinnvollerweise Artikel 8 Absatz 1 nDSG. Zu begrüssen ist, dass sie möglichst schlank und angesichts der stetigen technischen Entwicklungen flexibel, praxisnah und anwendungsfreundlich gehalten worden ist. Weil sie sehr allgemein formuliert ist, braucht es aber entsprechenden Deutungs- und Umsetzungshilfen für die Praxis.	- Es müssen seitens EDÖB möglichst bald Dokumente geschaffen werden, welche den Betrieben die Praxisumsetzung vereinfachen.
Art. 1 Abs. 2	Die Abstände zwischen den vorzunehmen Überprüfungen sollten präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Was genau „angemessene Abstände" sind, hängt selbstverständlich von den	[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen, jedoch

	Besonderheiten des konkreten Anwendungsfalls ab (S. 17 im erläuternden Bericht: «[…] bei der Bestimmung der Massnahmen selbstredend die Umstände des Einzelfalls massgeblich [bleiben]»). Während die Datenbearbeiter inhaltlich grossen Freiraum für die Bestimmung ihrer konkreten Massnahmen brauchen, sollte zeitlich zumindest eine konkrete Anforderung gelten, um die Sicherheit zu gewährleisten. Als sinnvoll erscheint uns eine mindestens jährliche Überprüfung.	mindestens einmal pro Jahr zu überprüfen.
Art. 2	Diese präzise Auflistung der Schutzziele macht Sinn: Sie stellt eine praxisorientierte ‚Gedächtnisstütze' für die Verantwortlichen und die Auftragsbearbeiter dar, was im Rahmen ihrer Konkretisierung zu berücksichtigen ist. Wichtig ist eine gute Anwendbarkeit in der Praxis (Seite 17 des Berichts: „In Anwendung der Verhältnismässigkeit sind ausgehend [… von dieser Auflistung der Schutzziele] die organisatorischen und technischen Massnahmen des Einzelfalls zu bestimmen."). Gleichzeitig zeigt diese Auflistung die Komplexität der Anforderungen an eine gesetzkonforme Datenbearbeitung und -sicherheit auf - mit dem damit verbundenen Aufwand. Aus diesem Grund ist eine möglichst konkrete und für Schweizer Betriebe auch unentgeltliche Unterstützung der Datenschutzverantwortlichen durch die zuständigen Behörden (insbesondere das EDÖB), vorzusehen. So können die Umsetzungskosten für Wirtschaft und Gesellschaft minimiert und angemessene Datensicherheit auf allen Ebenen geschaffen werden.	- Für eine optimale und kostengünstige Umsetzung ist darauf zu achten, dass Schweizer Unternehmen einen guten und kostengünstigen Zugang zum EDÖB erhalten (vgl. auch Art. 45 Abs. 2).
Art. 3	Welche „Massnahmen" im vorliegenden Rahmen berücksichtigt werden sollen und ob ein Risiko als hoch oder begrenzt eingeschätzt werden soll, dürfte in der Praxis oftmals schwierig zu beurteilen sein, denn Artikel 8 nDSG führt auch keine präziseren Anhaltspunkte über die Art der infrage stehenden Massnahmen an. Dies entspricht zwar einer flexiblen, bedarfsorientierten und dem neusten technischen Stand angepassten Umsetzung des Datenschutzes, macht aber dessen Realisierung in der Praxis schwierig. In diesem Sinne ist die Präzisierung der Inhalte der Protokollierung (gemäss Abs. 3) an sich konsequent und kongruent. Sie weist aber einen hohen Detaillierungsgrad auf, der einen entsprechend hohen Umsetzungsaufwand,	In Art. 3 Abs. 1 müssen Alternativen zur im Entwurf vorgesehenen (komplexen) Protokollierung – ausdrücklich vorgesehen und auch aufgezählt werden, namentlich Zugriffskontrollen, die physische/räumliche Sicherung der Daten, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.

	eine Unübersichtlichkeit und mögliche Verwechslungs-risiken mit sich bringt. Es ist festzustellen, dass gerade bei der *automatisierten* Bearbeitung von Personendaten die Anforderung einer detaillierten Protokollierung einen beträchtlichen Teil der Vorteile der Automatisierung beraubt: Der zeitliche und administrative Aufwand wird dadurch erheblich vergrössert. Trotzdem erscheint uns eine Protokollierung richtig, sofern keine anderen Massnahmen das gleiche Ziel mit weniger Aufwand erreichen können. *Antrag:* Alternativen zur Protokollierung als Massnahmen zum Datenschutz sollen im E-VDSG ausdrücklich vorgesehen und auch aufgezählt werden – wie etwa die physische/räumliche Sicherung der Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.	
Art. 4 Abs. 2	Weil in sehr vielen Fällen eine automatisierte Bearbeitung von besonders schützenswerten Personendaten erfolgt, sind die von dieser Bestimmung gestellten Anforderungen als zu aufwendig und vielfach unnötig zu qualifizieren. Sie bringen für die betroffenen Datenbearbeiter unangemessen hohe Kosten mit sich. Deswegen ist diese Auflistung zu kürzen. Die Buchstaben d, e und j sollen ersatzlos gestrichen werden, weil sie unnötige zusätzliche Anforderungen und Präzisierungen darstellen, die den administrativen Aufwand für die Betriebe verschärfen, ohne dass daraus ein entsprechender Nutzen entsteht. Buchstabe i soll gekürzt werden: Er weist einen Detaillierungsrad mit entsprechenden Umsetzungskosten auf, der in keinem vernünftigen Verhältnis zu seinem Nutzen steht. Hingegen werden Buchstaben a, b, c, f und g ausdrücklich begrüsst, da sie zentrale Massnahmen zur Gewährleistung der Datensicherheit darstellen. Ihre Einhaltung genügt, um dem Datenschutz gerecht zu werden. Auch Buchstabe h wird begrüsst, weil eine stets angestrebte Datenminimierung das beste Mittel darstellt, um sowohl den Schutz der Privatsphäre als auch die Verminderung des	[2] Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. ~~zur internen Organisation~~; e. ~~zur Herkunft der Personendaten und zur Art ihrer Beschaffung~~; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechti-gungen sowie zur Art

	mit jeglichem Datenbearbeitung verbundenen administrativen Aufwands zu erreichen.	und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den ~~Datenbearbeitungs-verfahren, insbesondere den~~ Verfahren bei der Speicherung, ~~Berichtigung, Bekanntgabe, Aufbe-wahrung, Archivierung,~~ Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. ~~zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.~~
Art. 4 Abs. 3	Analog obigem Antrag zu Art. 1 Abs. 2 sollten auch hier die zeitlichen Abstände zwischen den vorzunehmenden Aktualisierungen präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Deswegen wird hier beantragt, dass die Aktualisierungen mindestens einmal jährlich stattfinden: Dieser Zeitabstand stellt eine präzise, zugleich realistische und daher auch anwendungsfreund-liche Leitplanke dar.	[3] Die private Person muss das Reglement ~~regelmässig~~ in angemessenen Abständen, jedoch mindestens einmal pro Jahr, aktualisieren und der Datenschutzberaterin oder dem Datenschutz-berater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.
Art. 6 Abs. 2	Die in dieser Bestimmung gestellten Anforderungen an die Verantwortlichen betreffend dem DSG nicht unterstellten Datenbearbeiter sind offensichtlich zu hoch. Von einem Verantwortlichen kann vernünftigerweise nicht verlangt werden, dass er Kenntnis der vielen potenziell relevanten Gesetzesbestimmungen und der möglichen Abhilfe-Lösungen hat. Wenn schon ist es die Pflicht von Gesetzgeber und Verwaltung, den Datenschutz so auszugestalten, dass dieser – wo nötig und sinnvoll – überall für alle Betroffenen gleichermassen gilt. Diese Pflicht den einzelnen Verantwortlichen aufzubürden, wie der	~~[2] Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.~~

	Bundesrat es vorschlägt, führt zu enormer Unsicherheit und Aufwand. Deswegen ist dieser Absatz ersatzlos zu streichen.	
Art. 8 Abs. 1	Aus der Formulierung dieser Bestimmung geht überhaupt nicht klar hervor, wer für die Beurteilung der Angemessenheit des Datenschutzes in einem anderen Staat zuständig ist. Aus dem erläuternden Bericht hingegen schon (S. 25 ff): Der Bundesrat ist zuständig. Der Klarheit wegen sollte diese Zuständigkeit in Art. 8 E-VDSC eindeutig geregelt werden, sonst besteht das Risiko, dass sich private Akteure dafür verantwortlich halten – was ihren Aufwand erheblich erhöhen würde.	[1] Werden Personendaten ins Ausland bekanntgegeben, so müssen ~~bei der~~ anlässlich einer regelmässigen Beurteilung durch den Bundesrat, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden: […]
Art. 8 Abs. 3	Die Abstände zwischen den vorzunehmenden Beurteilungen sollen präziser angegeben werden. Deswegen wird auch hier beantragt, dass die Beurteilungen mindestens einmal jährlich stattfinden müssen.	[3] Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch, jedoch mindestens einmal pro Jahr, neu beurteilt.
Art. 9 Abs. 1	Die von Art. 9 E-VDSG gestellten Anforderungen erreichen ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Zwar sind diese Anforderungen für das Ziel des Datenschutzes konsequent, sie verursachen aber hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden. Nämlich Bst. b, c, g, h sowie i sind offensichtlich unnötig; Ihre Anwendung wäre unverhältnismässig aufwändig. Die anderen Bestimmungen genügen, um die «spezifischen Garantien» zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.	[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen die Datensicherheit mindestens die folgenden Punkte regeln: […] ~~b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen~~ ~~c. die Art und der Zweck der~~

		~~Bekanntgabe von Personendaten;~~ ~~[...]~~ ~~g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger;~~ ~~h. die Massnahmen zur Gewährleistung der Datensicherheit;~~ ~~i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;~~ [...]
Art. 10	Wir begrüssen, dass der EDÖB eine Liste von Standard-Datenschutzklauseln veröffentlicht, um den Aufwand für die Betroffenen zu reduzieren und eine gewisse Vereinheitlichung der Schutzklauseln zu erreichen.	-
Art. 15	Bei der Anwendung dieser Bestimmung ist darauf zu achten, dass die Anforderungen an den Detaillierungsgrad der mit der Bekanntgabe von Personendaten verbundenen Informationen nicht zu umfangreich ausfallen soll. Meistens werden sich die zum Datenschutz benötigten Informationen aus den Daten oder den Begleitumständen selbst ergeben.	-
Art. 18	Nach unserer Einschätzung reicht es aus, wenn *nach Beendigung der Datenbearbeitung* (was bei entsprechenden Gerichtsverfahren bereits Jahre dauern kann) eine Aufbewahrung für ein Jahr statt zwei Jahre stattfindet.	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während ~~zwei Jahren~~ einem Jahr nach Beendigung der Daten-bearbeitung aufbewahrt werden.
Art. 20	Die vorgesehene Dreifachlösung (schriftlich, mündlich oder durch Einsichtnahme an Ort und Stelle) erscheint sinnvoll. So kann für Menschen mit gewissen Krankheiten oder einer Beeinträchtigung eine geeignete Lösung gefunden werden.	[3] Die Auskunft muss für die betroffene Person verständlich sein, soweit dies im

	Für gewisse Fälle, wie an Demenz erkrankte oder weitere kognitiv beeinträchtigte Menschen dürfte die Anforderung in Abs. 3 kaum einzuhalten sein. Deshalb ist für diese Fälle eine Präzisierung aufzunehmen.	Rahmen ihrer kognitiven Fähigkeiten möglich ist.
Art. 22	Die Frist von 30 Tagen ab Eingang des Begehrens um Dateneinsicht erscheint uns vernünftig. Es stellt sich einzig die Frage, ob nicht die Gerichtsferien berücksichtigt werden sollten (namentlich die Sommermonate und Weihnachten, wegen vieler Absenzen).	
Art. 23	Bei unverhältnismässig aufwändigen Auskunftserteilungen erscheint uns die auf 300 Franken angesetzte Obergrenze als zu tief. Wenn damit mehrere Arbeitstage an Aufwand anfallen, wäre nicht einmal ein Bruchteil der Kosten auf die Gesuchstellenden gedeckt. Der Betrag sollte – auch gerade als Schutz vor querulatorischen Begehren – auf mindestens 1'000 Franken erhöht werden, um tatsächlich abschreckend wirken zu können.	[1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. [2] Die Beteiligung beträgt maximal ~~300~~ 1'000 Franken.
Art. 25	Die Datenschutzgesetzgebung weist eine hohe Komplexität auf; deshalb sind ihre Anforderungen in der Praxis nicht immer einfach einzuhalten. Deswegen ist es sehr sinnvoll, Datenschutzberatende einzusetzen und die konkreten Modalitäten zu deren Einsatz im Sinne dieser Bestimmung festzulegen. Die Inhalte sind zu begrüssen, wie sie in dieser Bestimmung vorgeschlagen sind.	-
Art. 26 Bst. a + b	Die hier definierte und sinnvolle Ausnahme einer Pflicht zur Führung eines Bearbeitungsverzeichnisses würde bei zahlreichen Betrieben nicht zur Anwendung kommen, weil • in vielen Fällen die Betriebe besonders schützenswerte Personendaten in grossem Umfang bearbeiten; • aus einer Interpretation von Art. 20 Abs. 4, Art. 26 Abs. 3, Art. 31 Abs. 2 Bst. b nDSG hervorgeht, dass Art. 26 eVSDG auch Betriebe mit weniger als 250 Mitarbeitenden angewendet werden soll, wenn sie einem Konzern zugehören, der insgesamt mindestens 250 Mitarbeitende beschäftigt. Um Rechtssicherheit zu gewährleisten und keinen unnötigen Aufwand für kleinere Betriebe (namentlich im Sozial- und Gesundheitsbereich) zu schaffen, ist eine	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:

	Anpassung wichtig. Während wir die Unterstellung von Teilen der Konzerne nachvollziehen können, erscheint uns die «Bearbeitung von besonders schützenswerten Daten in grossem Umfang» als zu wenig präzise Konkretisierung. Wir beantragen deshalb eine Präzisierung, was unter «grossem Umfang» zu verstehen ist, nach unserer Ansicht wäre die Schwelle etwa bei 1'000 Datensätzen festzusetzen. Diesfalls erhält auch die Führung eines Verzeichnisses aber auf freiwilliger Basis mehr Gewicht, sie kann insbesondere bei regelmässiger Bearbeitung von Personendaten eine nützliche und einfache Tätigkeitsunterstützung darstellen: Dadurch können das Beibehalten eines Überblicks der Bearbeitungstätigkeiten und auch die Einhaltung anderer Verpflichtungen erleichtert werden.	a. Es werden umfangreich (mindestens 1'000 Datensätze) besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.
Art. 45 Abs. 2	Aus unserer Sicht ist unverständlich, warum eine nationale Behörde für die Dienstleistung im Bereich des der ganzen Bevölkerung dienenden Datenschutzes solch hohe Kostensätze von 150 bis 350 Franken verlangen soll. Dies schreckt geradezu ab, diese sinnvollen Dienstleistungen zu beziehen, welche einer guten Umsetzung der Gesetzgebung dienen. Es ist unverständlich, dass für die Dienstleistungen der Verwaltung solche Preise wie bei spezialisierten Anwaltskanzleien verrechnet werden. Als besonders stossend empfinden wir solche Honorare zulasten von Leistungserbringern, wenn diese besonders schützenswerte Personendaten bearbeiten: Es wäre falsch, diese mit hohen Stundensätzen vom Bezug der sinnvollen Unterstützung seitens EDÖB abzuschrecken. Diese Betriebe sind denn mit den neuen Regelungen auch besonders stark herausgefordert und eine gute Umsetzung ist im Interesse der Behörden und der Bevölkerung. Diese Belastung ist umso fragwürdiger, als die öffentliche Hand im Endeffekt und in vielen Fällen, die dadurch verursachten Defizite ausgleichen soll: Mit einer Hand wegnehmen, was mit der anderen gegeben wird, macht betriebswirtschaftlich keinen Sinn und verursacht einen sinnlosen administrativen Aufwand. Die Zutrittsschwelle zum EDÖB ist niedrig zu halten, ganz besonders auch zur Überprüfung der Angemessenheit von Kodizes (Art. 59 Abs. 1 Bst. a nDSG) oder die Genehmigung von Standarddatenschutzklauseln (Art. 59 Abs. 1 Bst. b	[2bis] Wenn die Bearbeitung besonders schützenswerte Personendaten betrifft, wird auf die Erhebung von Kosten verzichtet. Alternativ: [2bis] Wenn die Bearbeitung besonders schützenswerte Personendaten betrifft, gilt ein Stundenansatz von 50 bis 100 Franken.

	nDSG). Im Sinne einer rechtmässigen Umsetzung der komplexen neuen Datenschutzgesetzgebung sollte das Anrufen des EDÖB nicht durch das Erheben von Gebühren entgegengewirkt werden. Ganz besonders für den Bereich der Gesundheitsbetriebe muss deshalb eine Ausnahme geschaffen werden, welche vernünftige Stundenansätze vorsieht.	

Wir danken Ihnen für die Gelegenheit zur Vernehmlassung und für die gebührende Berücksichtigung unserer Stellungnahme im Rahmen Ihrer weiteren Bearbeitung dieses Geschäfts.

Freundliche Grüsse

Peter Saxenhofer
Geschäftsführer
INSOS Schweiz

Tschoff Löw
Leiter Politik
INSOS Schweiz

Kontakt für Rückfragen:
Tschoff Löw
Tel. 031 385 33 06
tschoff.loew@insos.ch

ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données
Rue des Chanoines 2, 1700 Fribourg

Office fédéral de la justice
M. Jonas Amstutz
Bundesrain 20
3003 Berne
Courriel

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

La Commission

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08
www.fr.ch/atprd

Réf: LS 2021-PrD-225 et 2021-Trans-177
Courriel: secretariatatprd@fr.ch

Fribourg, le 11 octobre 2021

Avant-projet d'Ordonnance fédérale relative à la Loi fédérale sur la protection des données (OLPD)

Monsieur,

Nous nous référons au courrier du 23 juin 2021 du DFJP concernant l'objet cité en référence ainsi qu'au courriel du 5 octobre 2021 de la Chancellerie de l'Etat de Fribourg, qui nous propose de vous transmettre directement notre réponse à la consultation susmentionnée, et vous remercions de nous avoir consultés à ce sujet.

La Commission en a traité lors de sa séance du 31 août 2021. Elle ne se prononce que sur les aspects relatifs à la protection des données et à la transparence (art. 30*a* al. 1 let. b de la loi du 25 novembre 1994 sur la protection des données, LPrD ; art. 40 let. c de la loi du 9 septembre 2009 sur l'information et l'accès aux documents, LInf).

A toutes fins utiles, la Commission tient à relever que son examen se limite à vérifier la conformité des dispositions aux exigences des règles de protection des données et de transparence. Il ne lui appartient pas de rendre attentif sur les conséquences du respect des exigences, ni de vérifier si des traitements de données nécessitant une base légale auraient été oubliés.

I. Sous l'angle de la protection des données

La Commission salue l'inclusion dans une même partie des principes généraux tant pour les organes fédéraux que pour les personnes privées.

La Commission relève à regret que la complexité de la Loi fédérale du 25 septembre 2020 sur la protection des données révisée (ci-après : *n*LPD) n'est ni atténuée ni expliquée suffisamment par le projet de révision totale de l'Ordonnance relative à la Loi fédérale sur la protection des données (ci-après : *n*OLPD). Les modalités, voire les répercussions en cas de non-respect, demeurent pour l'essentiel floues (à titre d'exemple, la demande de réexamen de l'article 17 peut-elle conduire à une nouvelle décision ?). À notre sens, de nombreux instruments appellent quelques précisions. Prenons l'exemple de l'analyse d'impact, l'article

3 alinéa 1 explique que lorsqu'il résulte de celle-ci un risque élevé, une journalisation est nécessaire. Ce nonobstant, l'article 22 *n*LPD explique que le risque élevé mène à l'élaboration d'une analyse d'impact. Il ne s'agit ici que d'une des nombreuses contradictions présentent dans le projet.

Par ailleurs, le rapport explicatif (ci-après : « RE ») offre des explications qui gagneraient à être stipulées dans l'Ordonnance. Par souci d'uniformité, il se justifierait de trouver dans les textes de loi les obligations indispensables, et non dans les documents explicatifs (à titre d'exemple, concernant l'article 2, il est expliqué que « si un objectif n'est pas pertinent, les responsables du traitement et les sous-traitants doivent être en mesure de le justifier » (*cf.* RE, p. 17)).

Finalement, la complexité de la matière demande un texte de loi clair et pratique, notamment lorsqu'il est question de permettre et faciliter l'exécution de la loi. Ce faisant, nous nous référons, pour les détails, à la prise de position de privatim du 2 septembre 2021, annexée à la présente, qui fait partie intégrante de notre détermination.

II. Sous l'angle de la transparence

La Commission n'a aucune remarque à formuler concernant cette thématique.

Tout en vous souhaitant bonne réception de la présente, nous vous prions de recevoir, Monsieur, nos salutations les meilleures.

p.o. Flouguely
Laurent Schneuwly
Président

Annexe

—

Prise de position du 1er septembre 2021 de privatim relative à la révision totale de l'Ordonnance relative à la Loi fédérale sur la protection des données (OLPD)

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail:
jonas.amstutz@bj.admin.ch

Bern, 1. September 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassungsverfahren

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) Stellung nehmen zu können. Gerne äussern wir uns dazu wie folgt:

1. Allgemeines

Das revidierte Bundesgesetz über den Datenschutz vom 25.09.2020 (revDSG) beinhaltet zahlreiche Delegationsnormen, auf die sich der vorliegende E-VDSG stützt (siehe Ingress E-VDSG). Zudem konkretisiert der E-VDSG verschiedene Bestimmungen des revDSG.

Insgesamt entsteht der Eindruck einer Verordnung, die (zu) wenig Klarheit für die Umsetzung durch die Verantwortlichen schafft. Einerseits liegt es darin, dass überholte Begriffe und Bestimmungen der bisherigen Verordnung einfach übernommen werden. Andererseits bringen die neuen Bestimmungen nicht die notwendige Detaillierung für die Umsetzung des an sich schon komplexen revDSG.

Die Verantwortlichen – private Personen wie auch Bundesorgane – werden Mühe haben, verschiedene dieser Bestimmungen angemessen umzusetzen.

Das Konzept der E-VDSG und einzelne Bestimmungen sollten deshalb im Hinblick auf eine wirkungsvolle Umsetzung des Datenschutzes grundsätzlich überprüft werden.

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, CH-3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

2. Einzelne Bestimmungen

a. Art. 1 bis 4 E-VDSG (Datensicherheit)

Die Art. 1 bis 4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 revDSG). Dabei verlangt Art. 8 Abs. 3 revDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt.

Der E-VDSG verpasst es, diese Mindestanforderungen in einer Form zu konkretisieren, die auch in Bezug auf die strafbewehrte Unterlassung der Umsetzung der Mindestanforderungen (Art. 61 Abs. 1 Bst. c revDSG) objektive Tatbestandsmerkmale erkennen lassen würde. In Bezug auf die Datensicherheit ist in der Informationsbearbeitung heute ein Standard erreicht, der klar nach der Beurteilung des Schutzbedarfs und der Risiken die entsprechenden Sicherheitsmassnahmen vorschlägt und einteilt (Grundschutz, hoher Schutz, sehr hoher Schutz). Der Bund hat soeben mit der Verabschiedung des Bundesgesetzes über die Informationssicherheit (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020) gezeigt, wie die heutigen Anforderungen auch gesetzestechnisch umgesetzt werden können.

Der E-VDSG hält dagegen am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht, ohne aber Art. 8 revDSG für die Praxis zu konkretisieren.

Der Abschnitt 1 (Datensicherheit) ist aus unserer Sicht konzeptionell grundsätzlich zu überarbeiten.

b. Art. 1 E-VDSG

Art. 1 Abs. 1 E-VDSG schreibt eine Beurteilung der Angemessenheit von Massnahmen nach den Kriterien Zweck, Art, Umfang und Umstände der Datenbearbeitung, Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen, Stand der Technik und Implementierungskosten vor.

Hier wird im Wesentlichen Art. 32 DSGVO rezipiert, ohne aber das in diesem Artikel formulierte Ziel in den Vordergrund zu stellen: «ein dem Risiko angemessenes Schutzniveau zu gewährleisten».

Mitunter bedeutet dies, dass die Schutzziele, der Schutzbedarf und die Risiken zuerst zu beurteilen sind.

Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt, wie dies auch die Erläuterungen erwähnen (S. 15) und werden in Art. 2 E-VDSG ausführlich aufgezählt (siehe nachfolgend Art. 2 E-VDSG). Der Schutzbedarf ergibt sich aus der Art der Daten (Personendaten, besonders schützenswerte Personendaten) und der Datenbearbeitung selbst (z.B. Profiling). Erst dann erfolgt die Risikobeurteilung, wie dies auch die Datenschutz-Folgenabschätzung vorsieht (Art. 22 revDSG).

Die Kriterien «Zweck, Art, Umfang und Umstände der Datenbearbeitung» beziehen sich somit auf die Schutzbedarfsfeststellung (welche bereits eine erste grobe Einschätzung des möglichen Schadensausmasses enthält), die Kriterien «Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen» auf die Risikobeurteilung.

Wenn es um die Beurteilung der Angemessenheit der Massnahmen geht, sind die Kriterien «Stand der Technik und Implementierungskosten» einschlägig. Sie sagen aber nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche dem Risiko mit der nötigen Effektivität begegnet. Dies ist im erwähnten ISG so angelegt, aber auch in Art. 32 DSGVO, der hier zitiert wird (Erläuterungen, S. 15).

Art. 1 Abs. 1 E-VDSG ist deshalb konzeptionell grundsätzlich zu überarbeiten.

Art. 1 Abs. 2 E-VDSG verlangt, dass die Massnahmen über die gesamte Bearbeitungszeit in angemessenen Abständen zu überprüfen sind. Diese Formulierung greift zu kurz. In erster Linie ist die Risikobeurteilung laufend zu überprüfen, woraus sich die Massnahmen und deren Angemessenheit ergeben und somit die allfällige Anpassung von Massnahmen.

Die Formulierung ist zu korrigieren.

c. Art. 2 E-VDSG

Die Aufzählung der Schutzziele wurde aus der geltenden Verordnung übernommen und mit Bestimmungen aus der DSGVO ergänzt.

Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt und lassen sich in die in der Informatiksicherheit üblichen Schutzziele zusammenfassen: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit (so auch Erläuterungen, S. 15). Er erscheint als angezeigt, dies entsprechend klar zum Ausdruck zu bringen (vgl. in diesem Sinne Art. 6 Abs. 2 des Informationssicherheitsgesetzes vom 18.12.2020).

Die in Art. 2 aufgeführten Vorgaben stellen keine eigenständigen Schutzziele dar, sondern Anforderungen an die Massnahmen, welche zur Erreichung der Schutzziele zu treffen sind (so stellt etwa die Zugriffskontrolle kein Schutzziel dar, sondern eine Anforderung zur Gewährleistung der Vertraulichkeit im Rahmen des Verhältnismässigkeitsprinzips).

Zudem ist der Einleitungssatz von Art. 2 E-VDSG missverständlich. Schutzziele sind Zielvorgaben. Die Massnahmen müssen angemessen sein in Bezug auf die in der Risikobeurteilung festgestellten Risiken und nicht in Bezug auf die Schutzziele.

d. Art. 3 E-VDSG

Art. 3 E-VDSG sieht insbesondere für Bundesorgane eine ausführliche Protokollierung der Datenbearbeitungen vor.

Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und dann unter Umständen sanktioniert) werden kann. Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das mittels Protokollierung wirksam reduziert werden kann; dass ein *irgendwie* geartetes Risiko verbleibt, reicht nicht (es fehlt dann an der Verhältnismässigkeit der neuen Datenbearbeitung). Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen zu umfassende Berechtigungen implementiert werden müssen, weil nicht zum Vorherein bekannt ist, auf welche konkreten Daten

der/die Berechtigte bei der Aufgabenerfüllung Zugang haben muss (z.B. im Schengen-Informationssystem). Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert und stichprobenweise überprüft werden. Die Pflicht zur Protokollierung als kompensierende Massnahme ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert.

Für die Bundesorgane soll die Protokollierung für das Bearbeiten sämtlicher Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Hier wird weit über das Ziel hinausgeschossen. Die Protokollierung stellt selbst eine Beschaffung von Personendaten dar, die dem Grundsatz der Verhältnismässigkeit genügen muss. Zwar erlaubt Art. 57*l* Bst. b Ziff. 4 RVOG die Aufzeichnung von Randdaten zum Nachvollzug des Zugriffs auf Datensammlungen, aber eben nur insoweit, als die Aufzeichnung verhältnismässig ist. Dass selbst bei einfachen Personendaten und selbst bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht klar über diese Anforderung hinaus. Die Bundesorgane sind deshalb in Absatz 1 aufzunehmen und auf Absatz 2 ist zu verzichten.

In Art. 3 Abs. 3 E-VDSG sollte vor «die Identität der Empfängerin oder des Empfängers» das Wort «gegebenenfalls» eingefügt werden, da es sich nicht bei jeder protokollierten Bearbeitung um eine Bekanntgabe handelt.

Gemäss Art. 3 Abs. 4 E-VDSG sind die Protokolle während zweier Jahre aufzubewahren und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei ist nicht in jedem Fall eine personenbezogene Auswertung erforderlich. Für die Bundesorgane legen die Art. 57*m* ff. RVOG und Art. 8 ff. der zugehörigen Ausführungsverordnung fest, wie die Auswertungen erfolgen dürfen, wobei ggf. auch ein gestaffeltes Vorgehen angezeigt ist (vgl. BGE 143 II 443). Der letzte Satz ist deshalb im Sinne «dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden» zu ergänzen.

e. Art. 4 E-VDSG

Die Erstellung eines Bearbeitungsreglements wird für private Verantwortliche und deren Auftragsbearbeiter vorgesehen, die (1) umfangreich besonders schützenswerte Personendaten bearbeiten oder (2) ein Profiling mit hohem Risiko durchführen (Art. 4 Abs. 1 E-VDSG). Diese Eingrenzung erscheint willkürlich und deckt bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen ab.

Hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG). Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 revDSG), die Teil des Bearbeitungsreglements sein können.

Art. 4 Abs. 2 E-VDSG enthält Mindestangaben für das Datenbearbeitungsreglement. Auch hier wird kein Konnex zu den Standards in der Informatik gemacht, in dem auf diese verwiesen würde. Dann würde es genügen, auf die spezifischen datenschutzrechtlichen Vorgaben hinzuweisen (Bst. h, j).

Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater ist die Fachperson bei einem Verantwortlichen und ein Bearbeitungsreglement wird zusammen mit ihr/ihm erstellt und nicht «der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung» gestellt. Es gehört zu den Aufgaben der Datenschutzberaterin oder des Datenschutzberaters, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b revDSG). Zudem hat die Datenschutzberaterin oder der Datenschutzberater über die erforderlichen Fachkenntnisse zu verfügen (Art. 10 Abs. 3 Bst. c revDSG), weshalb die Formulierung, das Bearbeitungsreglement sei ihr oder ihm «in verständlicher Form» zur Verfügung zu stellen, offensichtlich eine Abwertung seiner Fachkompetenzen impliziert.

Art. 4 Abs. 3 E-VDSG ist ersatzlos zu streichen.

f. Art. 5 E-VDSG

Grundsätzlich kann auf unsere Ausführungen zu Art. 4 E-VDSG verwiesen werden.

g. Art. 7 E-VDSG

Auch die Datenschutzberaterin oder der Datenschutzberater des Bundesorgans hat bei der Anwendung der Datenschutzvorschriften mitzuwirken (vgl. unten Art. 28 E-VDSG). Es widerspricht dem präventiven und risikoorientierten Ansatz des revDSG, wenn die Datenschutzberaterin oder der Datenschutzberater lediglich nachträglich über den Abschluss eines Outsourcingvertrags oder bei einer Funktionsübertragung informiert werden soll. Zu den Aufgaben einer Datenschutzberaterin oder eines Datenschutzberaters gehört die Involvierung in solche Geschäfte. Die ist eine Kernaufgabe der Beraterin oder des Beraters («Mitwirkung bei der Anwendung der Datenschutzvorschriften»). Die Datenschutzberaterin oder der Datenschutzberater ist rechtzeitig zu informieren, wie dies korrekterweise bei Datenbearbeitungsprojekten vorgesehen ist (Art. 31 E-VDSG).

Art. 7 E-VDSG ist ersatzlos zu streichen.

h. Art. 8 E-VDSG

Bei den Formulierungen in Art. 8 E-VDSG fällt auf, dass der EDÖB konsultiert wird (formell), und die Beurteilungen von internationalen Organisationen oder ausländischen Behörden berücksichtigt werden können (materiell). Es ist klar zu formulieren, dass auch die Stellungnahmen des EDÖB materiell zu berücksichtigen sind, zumal sich die Erläuterungen hierzu nicht äussern (Erläuterungen, S. 27).

i. Art. 9 Abs. 3 E-VDSG

Gemäss Art. 16 Abs. 2 Bst. b und c revDSG sind Datenschutzklauseln und spezifische Garantien dem EDÖB vorgängig mitzuteilen. Der Einleitungssatz von Art. 9 Abs. 3 E-VDSG suggeriert, dass es einen Sachverhalt geben könnte, in der auch die Nicht-Mitteilung zu einer rechtskonformen Bekanntgabe ins Ausland führen würde.

Die Formulierung ist anzupassen.

j. Art. 19 E-VDSG

Art. 24 Abs. 1 revDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 revDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 revDSG).

Art. 24 revDSG ist eine (bewusst) abweichende Bestimmung von Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO rezipiert. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen. Für die Mehrheit der Verantwortlichen ist dies aber nicht der Fall und Art. 19 E-VDSG bringt unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde rasch informiert wird, allenfalls auch die betroffenen Personen, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden.

Art. 24 revDSG braucht die in Art. 19 E-VDSG enthaltene Konkretisierung nicht.

k. Art. 20 E-VDSG

Art. 25 revDSG und Art. 26 revDSG regeln das Auskunftsrecht und dessen Einschränkungen ausführlich. Art. 20 E-VDSG bringt hierzu einige Konkretisierungen, die aber über das Notwendige hinausgehen.

Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 revDSG definiert. Daraus ergeben sich der Umfang und der Zweck der Auskunft. Dies misst sich nach objektiven Kriterien. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte.

Art. 20 Abs. 3 E-VDSG ist ersatzlos zu streichen.

Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen». Dies ergibt sich bereits aus Art. 8 revDSG und den Bestimmungen des 1. Kapitels der E-VDSG.

Diese Erwähnung ist in Art. 20 Abs. 4 E-VDSG zu streichen.

Art. 26 Abs. 4 revDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person.

Art. 20 Abs. 5 E-VDSG ist ersatzlos zu streichen.

l. Art. 21 E-VDSG

Art. 21 Abs. 1 E-VDSG sieht vor, dass ein Verantwortlicher, der für die Behandlung des Begehrens nicht zuständig, dieses an den zuständigen Verantwortlichen weiterleitet. Dieser verwaltungsrechtliche Grundsatz gilt für die Bundesorgane auch ohne Erwähnung in diesem Zusammenhang. Im öffentlich-rechtlichen Bereich ergibt er sich aus dem hoheitlichen Verhältnis der Bürgerinnen und Bürger zum Staat. Im privatrechtlichen Verhältnis legen die Parteien ihre Rechte und Pflichten aber autonom fest. Die gleiche Auflage auch dem privatrechtlichen Verantwortlichen zu machen, ist unverhältnismässig. Sie führt zu einem Aufwand für den privatrechtlichen Verantwortlichen, den «zuständigen» Verantwortlichen ausfindig zu machen, ohne dass dadurch die Rechte der betroffenen Personen gestärkt würden.

Art. 21 Abs. 1, 2. Satz E-VDSG ist ersatzlos zu streichen.

m. Art. 24 E-VDSG

Art. 24 E-VDSG beinhaltet eine Konkretisierung von Art. 28 revDSG, indem er sich auf die sinngemässe Anwendung von Bestimmungen zum Auskunftsrecht verweist. Dies wird dem neuen Rechtsinstitut der «Datenportabilität» nicht gerecht und verkennt den durchaus vorhandenen Bedarf einer Konkretisierung der gesetzlichen Bestimmung (beispielsweise in Bezug auf die «gängigen elektronischen Formate» oder den «unverhältnismässigen Aufwand» bei der direkten Übertragung von einem Verantwortlichen zu einem anderen). Zudem wäre auch in Bezug auf die Ausnahmen der Kostenlosigkeit eine andere Regelung als beim Auskunftsrecht denkbar, da hier nicht der Persönlichkeitsschutz, sondern der wirtschaftliche Wert der Daten im Vordergrund steht.

Art. 24 E-VDSG ist vollständig zu überarbeiten.

n. Art. 25 E-VDSG

Art. 25 E-VDSG hält fest, welche Aufgaben die Datenschutzberaterin oder der Datenschutzberater wahrnehmen muss. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 revDSG, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die er oder sie wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 revDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist missverständlich und zu korrigieren.

o. Art. 26 E-VDSG

In Anwendung von Art. 12 Abs. 5 revDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn (1) umfangreich besonders schützenswerte Personendaten bearbeitet werden oder (2) ein Profiling mit hohem Risiko durchgeführt wird. Wie bei Art. 4 Abs. 1 E-VDSG ist zu erwähnen, dass diese Eingrenzung bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es angezeigt, die Voraussetzungen

für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG).

p. Art. 28 E-VDSG

Art. 28 E-VDSG legt die Aufgaben der Datenschutzberaterin oder -beraters der Bundesorgane fest. In der Aufzählung von Art. 28 Abs. 2 E-VDSG fällt auf, dass die in Art. 10 Abs. 2 Bst. b revDSG festgelegte Aufgabe – die Mitwirkung bei der Anwendung der Datenschutzvorschriften – nicht erwähnt wird, sondern nur die Schulung und Beratung (Art. 10 Abs. 2 Bst. a revDSG). Wir gehen davon aus, dass es sich hier um ein Versehen handelt, ist doch die Mitwirkung bei der Anwendung der Datenschutzvorschriften eine Kernaufgabe von Datenschutzberaterinnen und -berater. Diese Aufgabe ist in Art. 28 Abs. 2 E-VDSG zu ergänzen.

q. Art. 36 E-VDSG

Die Bestimmung ist überflüssig, weil sich diese Präzisierung bereits aus Art. 39 revDSG klar ergibt.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim

MIGROSBANK RAIFFEISEN Verband Schweizerischer Kantonalbanken Union des Banques Cantonales Suisses Unione delle Banche Cantonali Svizzere VSRB VA ABRS

die Inlandbanken

Eidgenössisches Justiz- und Polizeidepartement
EJPD
Frau Bundesrätin
Karin Keller-Sutter
Bundeshaus West
3003 Bern

jonas.amstutz@bj.admin.ch

Stellungnahme der Inlandbanken zur Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG);

14. Oktober 2021

Sehr geehrte Frau Bundesrätin

Sehr geehrter Herr Amstutz

Anlässlich der Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz lassen wir Ihnen hiermit die Stellungnahme der Inlandbanken zukommen.

Das totalrevidierte Datenschutzgesetz, welches der Bundesrat dem Parlament im Jahr 2017 unterbreitet hatte, wurde in der parlamentarischen Debatte intensiv und eingehend diskutiert. Erstes Ergebnis dieser vertieften Auseinandersetzung war die Aufteilung der Vorlage. So war die Übernahme der Anpassungen infolge neuer Bestimmungen des Europäischen Rechts im Bereich der Schengen-Verträge weitgehend unbestritten. In einem zweiten Schritt wollte sich das Parlament für die Totalrevision des Datenschutzgesetzes jedoch genügend Zeit lassen. Diese Aufteilung war bereits ein Indiz dafür, dass das Parlament einen grundlegenden Überarbeitungsbedarf des Entwurfs identifizierte. In der Folge setzten sich die Staatspolitischen Kommissionen intensiv und ausführlich mit der Vorlage auseinander. In mehreren Runden der Differenzbereinigung wurde sie bewusst entschlackt. Das Parlament legte den Fokus darauf, Anpassungen an die Bedürfnisse des Schweizer Wirtschaftsstandorts vorzunehmen sowie auf «Swiss Finishes», welche die Schweizer Unternehmen vor grosse Umsetzungsschwierigkeiten sowie die Äquivalenz mit dem EU-Recht in Frage gestellt hätten, zu verzichten. Die eidgenössischen Räte verabschiedeten in der Folge eine Vorlage, welche mit den Bestimmungen der EU kompatibel ist, das bisher geltende Schutzniveau nicht unterschreitet und die Innovationskraft der Schweizer Wirtschaft gewährleistet.

Die Inlandbanken sind der Ansicht, dass die verabschiedete Fassung des revidierten Datenschutzgesetzes in die Erarbeitung der ausführenden Verordnung ungenügend Eingang gefunden hat. Diverse Bestimmungen, die auf Gesetzesstufe bewusst gestrichen worden sind, wurden in der Verordnung wiederum aufgenommen. Des Weiteren beinhaltet die Verordnung nicht nur Ausführungsbestimmungen

zum Gesetz, sondern diverse Verschärfungen und zusätzliche Vorschriften, für die das Gesetz keine entsprechende Grundlage bietet. Vor diesem Hintergrund ist es aus Sicht der Inlandbanken unabdingbar, die Verordnung einer grundlegenden Überarbeitung zu unterziehen und an das revidierte Datenschutzgesetz anzupassen. Dabei ist den Intentionen des Parlaments, eine möglichst prinzipienbasierte und innovationskraftfördernde Vorlage zu erarbeiten, die auf unnötige Bürokratie verzichtet, zwingend Rechnung zu tragen.

Die Inlandbanken sehen in den folgenden Artikeln besonderen Bedarf zur Streichung bzw. Überarbeitung:

- Streichung von Bestimmungen, auf die entweder in Folge der Vernehmlassung zum Datenschutzgesetz oder im Zuge des Gesetzgebungsprozesses verzichtet wurde, wie beispielsweise Art. 3 (Protokollierung), Art. 4 (Bearbeitungsreglement) und Art. 16 (Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten).
- Präzisierung von Bestimmungen, um der Realität des Schweizer Wirtschaftsstandorts Rechnung zu tragen, wobei der Aufwand für die betroffenen Unternehmen möglichst geringgehalten werden soll, ohne dabei das Ziel des Anliegens aus den Augen zu verlieren, wie beispielsweise in Art. 2 (Schutzziele), Art. 13 (Modalitäten der Informationspflichten), Art. 19 (Meldung von Verletzungen der Datensicherheit) und Art. 25 Abs. 1 Bst. a (Aufgaben Datenschutzberater/in).

Für die detaillierten Ausführungen und Anpassungsvorschläge der Verordnungsbestimmungen verweisen wir auf die Stellungnahme der economiesuisse und Schweizerischen Bankiervereinigung, welche die Inlandbanken vollumfänglich mittragen.

Wir bitten Sie um Berücksichtigung unserer Anliegen und danken Ihnen für Ihre Bemühungen.

Freundliche Grüsse

Dr. Jürg Gutzwiller
Präsident
Verband Schweizer Regionalbanken

Manuel Kunzelmann
Präsident der Geschäftsleitung
Migros Bank AG

Prof. Dr. Pascal Gantenbein
Präsident des Verwaltungsrats a.i.
Raiffeisen Schweiz Genossenschaft

Prof. Dr. Urs Müller
Präsident
Verband Schweizerischer Kantonalbanken

Beat Lehmann
Lic.iur. Füsprech
Acting Counsel Alcan Holdings Switzerland AG
Kongoweg 9 (Home Office)
5034 Suhr
E-Mail b.lehmann-aarau@bluewin.ch

Suhr, 14. Oktober 2021

Stellungnahme

zur

Totalrevision der Verordnung

zum Bundesgesetz über den Datenschutz

I Vorbemerkungen

1.1 Ausgangspunkt ist die Tätigkeit des Unterzeichnenden als Rechtskonsulent der IBM Schweiz (Zürich). und Europa (Paris) von 1969-1979, somit als Anbieter von Informatik-Produkten und Dienstleistungen; anschliessend im Konzernstab Recht der Alusuisse-Lonza Gruppe als Anwender der Informatik in einem weltweit tätigen Unternehmen.

1.2 In dieser Eigenschaft Berufung in die Expertengruppe des Bundesrates zur Vorbereitung des noch geltenden Datenschutzgesetze von 1992 (”DSG-1992”), aber auch zur Schaffung der Rechtsgrundlagen für die Führung und Aufbewahrung maschinell lesbarer Geschäftsunterlagen (heute Art. 958f und Geschäftsbücherverordnung - ”GeBüV”).

1.3 Dies har die Mitgliedschaft der juristischen Kommission verschiedenen Informatik-Fachorganisationen mit sich gezogen, namentlich im Wirtschaftsverband swico, der Vereinigung zum Unternehmensdatenschutz (VUD) und zur Informatiksicherheit (ISSS) sowie im Verband der Maschinen-, Elektro- und Metall-Industrie (swissmem)

1.4 Aufgrund des Meinungsaustausches mit Kollegen der erwähnten Fachorganisationen entstand die nachstehende Stellungnahme, die sich bewusst auf die Angelegenheit der Datensicherheit aus der Sicht privater Verantwortlicher (Unternehmen; Vereine; stiftungen) beschränkt

II Übergeordnete Zielsetzungen

Nach der vom Unterzeichnenden vertretenen Auffassung ist von folgenden übergeordneten Zielsetzungen für die Regelungen in DSG 2019 und E-VDSG auszugehen:

2.1 Anpassung er Datenschutzgesetzgebung an die rasch fortschreitende **Entwicklung der Informatik** und der Sicherheitsrisiken für die Bearbeitung von Personendaten**,** was eine Offenheit der Regelungen voraussetzt.

2.2 Aufrechterhaltung der **Konformität** mit dem harmonisierten europäischen Datenschutzrecht [Art. 45 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=DE

2.3 Möglichst weitgehender **Verzicht** auf Regelungen zu Datenschutz und Datensicherheit in unserem Land, welche im Sinne eines sog. *"**Swiss Finish**"* weiter gehen als die Bestimmungen der DSGVO

2.4 Ermöglichung der Umsetzung der Regelungen von DSG 2019 und E VDSG nicht nur durch die grösseren Unternehmen unseres Landes mit weltweiter Tätigkeit und oft einer Unternehmens-internen Organisation zu Gewährleistung von Datenschutz und Datensicherheit, sondern auch durch die hunderttausende von kleinen und mittleren Unternehmen ("**KMU**"), **Vereine** und **Stiftungen**.

2.5 DSG und VDSG sollten nach hier vertretener Auffassung in die sie **umgebende Rechtsordnung eingebettet** werden, mit dem Ziel der Harmonisierung zwecks Vermeidung von Redundanzen und Widersprüchen. Das gilt für den in Art. 2 Abs. 1 DSG-2020 umschriebenen **persönlichen Geltungsbereich**:

A. Bundesorgane

Regeln über den Umgang mit (maschinell lesbaren) Informationen durch die (Bundes-) Verwaltung, wie sie namentlich in folgenden Rechtsgrundlagen festgelegt sind

- **a.** Verordnung vom 30. November 2012 über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung) SR 172.010.441
- **b.** Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV) - SR 172.010.58
- **c.** Verordnung über das Informationssystem E-VERA, VEVERA - SR 235.22
- **d.** Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung) – SR 360.2

B. Private Personen

Diesbezüglich ist an die Anforderungen für die Bearbeitung und Aufbewahrung von Daten und Unterlagen durch die private Unternehmen zu denken, die in Art. 958f OR und der GeBüV enthalten sind, aber auch in den zahlreichen Aufzeichnungs- und Dokumentationspflichten im Steuerrecht und im Wirtschafts-Verwaltungsrecht.

III Anmerkungen zu den einzelnen Bestimmungen der E-VDG

3.1 Art. 1 Grundsätze – Absatz 2 (neu)

Auch an dieser Stelle könnte wie folgt auf die anzustrebende Konformität mit dem Stand des Datenschutzes und der Informatiksicherheit im EWR hingewiesen werden:

” Die technischen und organisatorischen Massnahmen sollten auf die internationale Entwicklung, insbesondere das harmonisierte europäische Datenschutzrecht und Datensicherungsniveau abgestimmt werden.“

3.2 Art. 1 Grundsätze - Absatz 2: ”Archivdaten“

Es wird darauf hingewiesen, dass es sich beim überwiegenden Teil der heute in Wirtschaft und Verwaltung vorhandenen lesbaren Informationen um **Archivdaten** handelt. Nach hier vertretener Auffassung sind diese Archivdaten in der Regel in redundanter Art und Weise auf einem unveränderbaren Datenträger im Sinne von Art 9 Abs. 1 Bst. a) GeBüV gespeichert. Unter dieser Voraussetzung sind die Archivdaten lediglich gemäss Art. 10 Abs. 1 GeBüV regelmässig auf Integrität und Lesbarkeit zu prüfen, ohne dass die Überprüfung auch die technischen und organisatorischen Massnahmen nach Art. 1 Abs. 1 E-VDSG umfassen muss. Dies könnte man in geeigneter Art und Weise in den Unterlagen zur Rev VDSG zum Ausdruck bringen.

3.3 Art. 2 Schutzziele – Abs. 1 ”Im Allgemeinen” (neu)

Es wird empfohlen, in einem ersten Absatz die zu erreichenden Schutzziele allgemein zu umschreiben:

a. Einhaltung der **Vertraulichkeit** der bearbeiteten Personendaten: Schutz vor dem Zugriff durch Unberechtigte;
b. Gewährleistung der **Integrität**: Echtheit und Unverfälschbarkeit (vgl. Art 3 GeBüV); und
c. Sicherung der **Verfügbarkeit** für die Berechtigten (vgl. Art. 6 und Art. 10 Abs. 2 Bst. b) GeBüV)

3.4 Art. 2 Schutzziele - Abs. 2 ”Mittel zur Umsetzung der Ziele“ (neu)

Es wird empfohlen, vor Auflistung empfohlener Massnahmen in einer generellen Klausel darauf hinzuweisen, welche organisatorischen und technischen Massnahmen den Verantwortlichen oder Auftragsbearbeitern für das Erreichen der Schutzziele zur Verfügung stehen, wo geeignete Mittel erfasst und verfügbar sind sowie aufgefunden und bgerufen werden können

” Zu diesem Zweck sollten die nach dem Stand der Technik verfügbaren und auf die erkannten Risiken abgestimmten technischen und organisatorischen Massnahmen im Sinne von Art. 7 DSG angewendet werden, die namentlich in folgenden vom EDÖB gesammelten und publizierten Grundlagen enthalten sein können:

a. vom EDÖB veröffentlichten **Verhaltenskodizes** von Berufs-, Branchen- und Wirtschaftsverbänden gemäss Art. 11 DSG;
b. die vom EDÖB gestützt auf Art. 58 DSG herausgegebene **Empfehlungen** zur Datensicherheit;
c. vom nationalen Zentrums für **Cybersicherheit** (NCSC) publizierten Richtlinien;
d. Empfehlungen von Einrichtungen der **Wissenschaft** sowie vom EDÖB anerkannten national oder international tätiger **Fachorganisationen** zur Datensicherheit (z.B. ENISA) gemäss Anhang I;
e. Liste der vom EDÖB genehmigten **Kontrollen** gemäss Anhang II. ”

3.4 Art. 2 Schutzziele – Abs. 3 ”Geeignete Mittel”

In einem weiteren Umsatz könnte, in Anlehnung an die Regelungen in der DSGVO auf die zum Erreichen der Schutzziele geeigneten Mittel hingewiesen werden

” Die auf das Risiko für die Daten abgestimmte Verschlüsselung sowie die Anonymisierung oder Pseudonymisierung der Daten können das Erreichen der Schutzziele ermöglichen. “

3.5 Art. 2 - Liste der ”Kontrollen”

3.5.1 Zur Auflistung der ”Kontrollen“ liesse sich in Abwandlung einer Arie des Fliegenden Holländer sagen ”*Wie aus der Ferne längst vergang'ner Zeiten spricht dieser Liste Text zu mir*”, oder Faust I, 1972-1973 ”*Es erben sich Gesetz’ und Rechte Wie eine ew’ge Krankheit fort …*”

3.5.2 Denn die Liste der damals ”10 Kontrollen“ fand sich bereits in der Anlage zu § 6 Bundesdatenschutzgesetz vom 17.01.1977 und gab den Stand der Datenverarbeitung aus der Mitte der 1970er Jahre wieder. https://www.bgbl.de/xaver/bgbl/start.xav?start=//*%5B@attr_id=%27bgbl177i0201.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl177s0201.pdf%27%5D__1634213961792

3.5.3 Verschiedene Regelungen wie die ”Zugangskontrolle zu EDV-Anlagen“, die Vorstellung von (physisch gedachte) ”Datenträgern” und deren ”Transport“ erscheinen unter den heutigen Bedingungen für den praktischen Einsatz der Informatik wie Schaustücke aus dem ”Technorama”: Vgl. einige willkürlich ausgewählte Stichworte: Datenverarbeitung in der ”Cloud”; ”Ubiquitäres”, ”Pervasives” und ”Wearable“ Computing; Digitalisierung der Kommunikation; Smart Phones; Dash Cams; Big Data; Künstliche Intelligenz; Internet und Internet der Dinge usw.)

3.5.4 Quelle der vorgeschlagenen Regelung von Art. 2 E-VDSG ist erkennbar Art. 29 ”Sicherheit der Verarbeitung“ der Richtlinie (EU) 2016/680 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX%3A32016L0680&rid=1 welche dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen **Behörden** zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von **Straftaten** oder der **Strafvollstreckung** dient**.**

Die Übernahme dieses Kataloges in die VDSG welche ganz allgemein der Umsetzung des Schutzes natürlicher Personen durch sämtliche Behörden (des Bundes) sowie privater Personen dient, ist sachfremd und vollumfänglich abzulehnen. ”*Sedes Materiae*” der betreffenden Regelung wäre nach hier vertretener Aufssung am ehesten eine Regelung unter dem SR Titel ”36 - Polizeikoodination und Dienstleistungen”.

3.5.5 Darüber hinaus erscheint besonders stossend, dass der Katalog **absolute Pflichten** aufstellt wie ”verwehrt, verhindert, verunmöglicht“ und damit den Anschein erweckt, dass bei Einhaltung diesen Massnahmen die Schutzziele umfassend realisiert werden können: Absolute Datensicherheit während unbestimmter zeit aber kann nicht hergestellt werden; wer sie sucht, findet Verzweiflung [Ausspruch meines ehemaligen IBM Kollegen Prof. Dr. K. Nagel http://www.prof-nagel.de ”Wer absolute (Daten-) Si-

cherheit sucht findet Verzweiflung!“ Hingegen erscheint der Katalog als geeignete Orientierungshilfe, welche Massnahmen im Hinblick auf das Erreichen des Schutzziels geeignet sein könen.

Wir schlagen vor, dass der Katalog in einem Anhang zur VDSG als **Checklist** für Punkte, welche bei der Realisierung eines Datensicherheitskonzepts zu prüfen sind aufgenommen werden könnte.

3.6 **Art. 3 und 4 - Bearbeitungsreglement und Protokollierung**

Diese Regelungen wurden vermutlich ebenfalls aus **der** Richtlinie (EU) 2016/680 in den Entwurf er VDSG übernommen. Es fehlt dazu nicht nur die Rechtsgrundlage, sondern sie sin insbesondere für die Datenbearbeitung durch private Personen (Unternehmen insbesondee KMU; Vereine; Stiftungen) viel zu weitgehend und tragen zur Datensicherheit nicht bei und sind ersatzlos zu streichen.

Suhr, im Home Office, 14. Oktober 2021

Beat Lehmann

Orientierungskopie an

- swico
- VUD
- ISSS
- swissmem

Migros-Genossenschafts-Bund
Direktion Legal & Compliance

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per mail an: jonas.amstutz@bj.admin.ch

Ort/Datum Zürich, 12. Oktober 2021
Betreff **Stellungnahme zum Vorentwurf Verordnung zum Datenschutzgesetz (VE-VDSG)**
Unsere Ref. R202149761

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf das Vernehmlassungsverfahren zum Vorentwurf für eine Verordnung zum Bundesgesetz über den Datenschutz (**VE-VDSG**) und danken Ihnen, dass Sie uns die Möglichkeit einer Stellungnahme dazu einräumen.

Der Migros-Genossenschafts-Bund (**Migros**) engagiert sich im Verein Unternehmens-Datenschutz (**VUD**), der eine detaillierte Stellungnahme zum VE-VDSG eingereicht hat. Wir verzichten deshalb auf eine eigene ausführliche Stellungnahme und beschränken uns nachfolgend auf ausgewählte Punkte. Im Übrigen schliessen wir uns der Stellungnahme des VUD vom 13. September 2021 vollumfänglich an.

Allgemeine Anmerkungen

Der Vorentwurf schiesst weit übers Ziel hinaus und schafft - vielfach ohne gesetzliche Grundlage - neue Pflichten, die teils sogar noch über die bereits strengen Anforderungen der Europäischen Datenschutz-Grundverordnung (**DSGVO**) hinausgehen. Der Vorentwurf bedarf einer grundlegenden Überarbeitung:

- Die Datenschutzverordnung muss sich auf jene Punkte beschränken, für die das revidierte Datenschutzgesetz effektiv Ausführungsvorschriften auf Verordnungsstufe vorsieht. Im Zusammenhang mit der Datenbearbeitung durch Private ist das im Wesentlichen mit Bezug auf die Datensicherheit (Mindestanforderungen), das Verzeichnis der Bearbeitungstätigkeiten (Ausnahmen für KMUs) und das Auskunftsrecht (Ausnahmen von der Kostenlosigkeit) der Fall. Es geht nicht an, auf dem Verordnungsweg neue Pflichten einzuführen, die keine gesetzliche Grundlage haben, zumal das revidierte Datenschutzgesetz das Ergebnis eines langen politischen Prozesses ist.

Migros-Genossenschafts-Bund
Direktion Legal & Compliance
Limmatstrasse 152
Postfach 1766
CH-8031 Zürich

Direktwahl +41 58 570 24 62
Zentrale +41 44 277 21 11
matthias.glatthaar@mgb.ch
www.migros.ch

Mwst-Nr. 231 115
Postcheckkonto 80-766-6

- Regelungen der heutigen VDSG dürfen nicht unbesehen fortgeschrieben werden, sondern es ist jeweils zu fragen, ob sie weiterhin sinnvoll sind - vor allem wenn sie zu einer Verschärfung im Vergleich zur DSGVO führen würden. Das revidierte DSG übernimmt viele Regelungen der Europäischen Datenschutz-Grundverordnung, die sich von jenen des heute geltenden Datenschutzgesetzes häufig auch konzeptionell unterscheiden. Dem gilt es auch bei Erlass der Datenschutzverordnung Rechnung zu tragen.

- Auf Verschärfungen im Vergleich zur DSGVO ist generell zu verzichten. Es war die erklärte Absicht des Gesetzgebers, Schweizer Unternehmen nicht strengeren Anforderungen zu unterwerfen als auf im EWR domizilierte Unternehmen anwendbar sind. Dies ist zu respektieren. Es ist wirtschaftspolitisch verfehlt (und rechtsstaatlich bedenklich), auf dem Verordnungsweg einen Wettbewerbsnachteil für Schweizer Unternehmen zu schaffen.

Anträge zu einzelnen Artikeln

Art. 2 (Datensicherheit/Schutzziele): Überarbeiten und an DSGVO angleichen
Der Katalog an Schutzzielen ist ausufernd und weicht in konzeptioneller Hinsicht von der Regelung der DSGVO ab. Zudem spricht der Verordnungstext absolut von "erreichen" und verkennt, dass es angesichts heutiger Cyberrisiken nicht realistisch ist, die Schutzziele stets zu erfüllen. Das ist umso kritischer, als die Verletzung der Mindestanforderungen an die Datensicherheit mit Strafe bedroht ist (Art. 61 lit. c revDSG). Die Mindestanforderungen an die Datensicherheit sind grundlegend zu überarbeiten und sollten an die zweckmässige Regelung von Art. 32 DSGVO angeglichen werden, die auf die anerkannten Schutzziele von Vertraulichkeit, Integrität und Verfügbarkeit fokussiert.

Art. 3 (Protokollierung): Streichen
Der Protokollierungspflicht fehlt eine gesetzliche Grundlage, zudem ist das Ergebnis einer Datenschutz-Folgenabschätzung kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. Auch ist die harte Zweckbindung und Zugriffsbeschränkung verfehlt: Wenn es in den Datenschutzhinweisen transparent beschrieben ist, spricht nichts dagegen, dass Log-Dateien z.B. auch für Analysezwecke ausgewertet werden.

Art. 4 (Bearbeitungsreglement): Streichen
Viele Unternehmen werden von sich aus ihre Datenbearbeitungen betriebsintern reglementieren. Auf eine verbindliche Vorschrift zur Führung eines Bearbeitungsreglements ist aber zu verzichten. Sie hat keine gesetzliche Grundlage. Sie ist auch ein "Swiss Finish"; die DSGVO kennt kein Bearbeitungsreglement. Unternehmen in der Schweiz sollten nicht mehr Dokumente erstellen müssen als Unternehmen im EWR. Schon das Erstellen und fortlaufende Pflegen der aus der DSGVO übernommenen umfangreichen Dokumentationen (Verarbeitungsverzeichnis, Datenschutz-Folgen-abschätzungen etc.) ist für Unternehmen enorm aufwändig. Von Schweizer Unternehmen zusätzlich die Erstellung weiterer Dokumente zu verlangen, ist unsinnig und für viele Unternehmen auch schlicht nicht realisierbar.

Art. 3 Abs. 4, Art. 18 Abs. 5, Art. 19 Abs. 5, Art. 20 Abs. 5 (Dokumentationspflichten): Streichen
Unternehmen werden häufig aus eigenem Interesse ihre Prozesse und Abwägungen dokumentieren. Es geht aber nicht an, solche Dokumentationen ohne gesetzliche Grundlage in der Verordnung verbindlich vorzuschreiben. Die Dokumentationspflichten sind auch ein "Swiss Finish". Auch hier gilt, dass Unternehmen in der Schweiz nicht mehr Dokumentationen führen müssen sollten als Unternehmen im EWR.

Art. 13 Abs. 1 (Modalitäten der Informationspflichten):
- Die Erwähnung des Auftragsbearbeiters ist zu streichen. Nach klarer Gesetzvorschrift hat nur der Verantwortliche eine Informationspflicht gegenüber betroffenen Personen (Art. 19 Abs. 1 revDSG). Der Auftragsbearbeiter hat selbst keine Informationspflicht und eine solche kann auch über die Verordnung nicht geschaffen werden.
- Es sollte eine zeitgemässe Regelung getroffen und festgehalten werden, dass über eine Webseite wirksam informiert werden kann, und zwar auch ohne Bereitstellung von Basisinformationen in der Verweisquelle.

Art. 13 Abs. 2 (Piktogramme): Streichen
Die Migros hat ein Privacy Icons Dashboard implementiert, das es Kund*innen erlaubt, sich schnell und einfach ein Bild davon zu machen, wie und wofür ihre Personendaten bearbeitet werden. Das Dashboard findet bei Kund*innen sehr guten Anklang. Eine Vorgabe, wonach Piktogramme in nicht näher spezifizierter Weise "maschinenlesbar" sein sollen, würde erhebliche Rechtsunsicherheiten bezüglich solcher Implementierungen schaffen. Sie könnte Unternehmen sogar davon abhalten, ähnliche kundenfreundliche Features umzusetzen, zumal die Vorschrift als Konkretisierung der strafbewehrten Informationspflicht konzipiert ist. Ein Unternehmen würde wohl eher von einer Nutzung von Piktogrammen ganz absehen, als Gefahr zu laufen, sich potenziell wegen nicht hinreichender "Maschinenlesbarkeit" einer Strafbarkeit auszusetzen. Das wäre ein rechtspolitisch unerwünschtes Ergebnis. Auch dieser Bestimmung fehlt zudem eine gesetzliche Grundlage. Sie ist ersatzlos zu streichen.

Im Übrigen verweisen wir auch auf die Stellungnahme des Vereins Privacy Icons vom 2. September 2021. Migros ist ein Mitglied des Vereins Privacy Icons und unterstützt dessen Stellungnahme.

Art. 15 (Information bei der Bekanntgabe von Personendaten): Streichen
Die Pflicht, Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der bekanntgegebenen Personendaten zu informieren, ist unsinnig, nicht umsetzbar und hat keine Grundlage im Gesetz. Daran ändert auch nichts, dass eine ähnliche Vorschrift in der heutigen Datenschutzverordnung enthalten ist. Die Bestimmung ist ersatzlos zu streichen.

Art. 16 (Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten): Streichen
Die Pflicht, Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren, widerspricht dem Willen des Gesetzgebers. Eine solche Pflicht war im

Vorentwurf des Datenschutzgesetzes enthalten, wurde im Gesetzgebungsprozess aber gestrichen. Nicht nachvollziehbar ist zudem die Erwähnung auch der "Einschränkung der Bearbeitung". Der Begriff entstammt der DSGVO; das revidierte Datenschutzgesetz kennt hingegen kein entsprechendes Recht betroffener Personen.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassungseingabe und stehen Ihnen bei Rückfragen gerne zur Verfügung.

Freundliche Grüsse
Migros-Genossenschafts-Bund

Matthias Glatthaar
Leiter Datenschutz & Digitalisierung

Jürg Maurer
Stv. Leiter Direktion Wirtschaftspolitik

PBS PRIVATE BILDUNG SCHWEIZ
SWISS PRIVATE EDUCATION
EDUCATION PRIVÉE SUISSE
EDUCAZIONE PRIVATA SVIZZERA

Per E-Mail:

jonas.amstutz@bj.admin.ch

Bern, 14. Oktober 2021 Fi/jf

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) Stellung nehmen zu dürfen.

Private Bildung Schweiz PBS vertritt auf nationaler Ebene die Interessen des Privatschulwesens. Betriebswirtschaftlich sind die Privatschulen überwiegend KMUs, die auf gute staatliche Rahmenbedingungen angewiesen sind. Wir sind daher für Lösungen, welche sich mit verhältnismässigem Aufwand umsetzen lassen und dabei auf die personellen und finanziellen Ressourcen der unterschiedlichen Schulen Rücksicht nimmt.

A. Das VDSG als Instrument zur Erreichung der Euro-Kompatibilität

Wie beim DSG hat der Bundesrat auch beim E-VDSG in seinen Erläuterungen festgehalten, dass es lediglich um die Angemessenheit des schweizerischen Datenschutzrechts im Vergleich zur europäischen DSGVO geht. In keiner Art und Weise wurde je von einer Erweiterung der Einschränkungen bei den Datenbearbeitungen bzw. von einer strengeren Regelung gesprochen. Diesem Ziel bleibt der Bundesrat auch bei der Formulierung der VDSG ausdrücklich verpflichtet. Alle Bestimmungen, welche folglich über die Erfordernisse der DSGVO hinausgehen, müssen als zweckfremd und als unzulässig abgelehnt werden. Diese sind konsequent aus dem E-VDSG zu löschen.

B. Formelle Bemerkung

Zur besseren Lesbarkeit der Verordnung und zum klareren Bezug zum DSG würden wir klare Verweise auf die betroffenen Gesetzesbestimmungen im Titel der jeweiligen Bestimmungen begrüssen.

C. Zu den einzelnen Bestimmungen

Art. 1 Abs. 1 Bst. d

In Art. 1 Bst. d werden als Kriterium der Angemessenheit für die Datensicherheit die «Implementierungskosten» genannt. Es wird begrüsst, dass der Aufwand für die Verantwortlichen auch ausdrücklich in die Angemessenheitsüberprüfung aufgenommen wird. Der verwendete Begriff erscheint jedoch problematisch, da er lediglich auf die geldwerten Umsetzungsaufwendungen beschränkt werden könnte (siehe auch S. 16 der Erläuterungen). Für eine solche Einschränkung gibt es keinen Grund. Statt den Begriff «Implementierungskosten» schlagen wir vor, den allgemeineren Begriff «Aufwand für den Verantwortlichen» zu verwenden. Es gibt keinen Grund, beim Verantwortlichen überhöhte Planungs- oder Projektkosten auszulösen, nur um festzustellen, ob die Implementierung dann ihrerseits verhältnismässig ist.

Art. 1 Abs. 2

Diese Bestimmung verlangt die Überprüfung der technischen und organisatorischen Massnahmen in angemessenen Abständen (gemeint sind hier die zeitlichen Abstände). Aufgrund des risikobasierten Ansatzes der gesamten Thematik der Datensicherheit erscheint diese Regelung falsch. Zudem ist fraglich, ob mit der vom Bundesrat aufgestellten Forderung der Überprüfung in angemessenen Abständen die Delegationsnorm von Art. 8 Abs. 3 DSG eingehalten wird. Die Mindestanforderungen an die Datensicherheit rechtfertigen keine Einführung von zusätzlichen Kriterien, welche im Gesetz nicht verankert sind. Es ist - wenn überhaupt - in materieller Hinsicht zu fordern, dass ein Zusammenhang zwischen der Überprüfung der Datensicherheit und der Entwicklung des Risikos hergestellt wird.

➔ Formulierungsvorschlag: «Die Massnahmen sind bei einer relevanten Veränderung des Risikos zu überprüfen.»

Art. 2 Einleitungssatz

Die Bestimmung spricht von «Schutzzielen erreichen». Die Pannen der Swisscom zeigen mit aller Deutlichkeit auf: Die absolute Datensicherheit gibt es nicht. Von den Verantwortlichen zu verlangen, dass die entsprechenden Schutzziele erreicht werden, ist weder korrekt noch realistisch. Der Bereich der Datensicherheit ist ein typischer Bereich, bei welchem keine Ergebnisverantwortung, sondern nur eine Sorgfaltspflicht auferlegt werden darf.

➔ Formulierungsvorschlag: «Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele anstreben: (…)»

Nur so dürfen in der nachfolgenden Aufzählung Begriffe wie «verwehrt», «verunmöglicht», «verhindert», «gewährleistet», usw. überhaupt verwendet werden. Ansonsten müssten in der Aufzählung die Schutzziele jeweils vernünftig relativiert werden.

Art. 2 Bst. a bis k

Art. 2 dürfte eigentlich nur Schutzziele nennen, welche vom Verantwortlichen beeinflusst werden können. Gerade die Transportkontrolle kann beispielsweise durch viele externe Faktoren

gefährdet werden, für welche der Verantwortliche nicht einstehen kann. Die Aufzählung von Art. 2 Bst. a bis k zeigt, was in der Lehre verschiedentlich moniert worden ist: Mangels Effizienz der staatlichen Interventionen, wird die Last der «Privacy by design» vollumfänglich auf den Verantwortlichen abgewälzt, statt dass sie zu datenschutzfreundlichen Technologien durch die Hersteller von Hard- und Software führen würde. Diese Entwicklung zulasten der Nutzer von Informationstechnologien ist problematisch, da damit auch der Aufwand für die Datensicherheit dem Betreiber und nicht dem Entwickler von Informationstechnologien auferlegt wird. Die Aufzählung in Art. 2 Bst. a bis k ist in Beachtung dieser Problematik zu überarbeiten und dem Verantwortlichen dürfen nur Schutzziele auferlegt werden, die auch tatsächlich in seiner Verantwortung liegen.

Art. 3

Die nun in der Verordnung vorgesehenen Anforderungen an die Protokollierung übersteigen das vernünftige Mass und führen zu einer Bürokratie, welche in keinem Verhältnis zum tatsächlichen Nutzen der Anforderungen steht. Insbesondere die Aufbewahrungsdauer der Protokolle von 2 Jahren (Art. 3 Abs. 4 E-VDSG) ist unangemessen. Aus Sicht der Wirtschaft genügt die Pflicht zur Erstellung eines Verzeichnisses der Datenbearbeitungen vollumfänglich, um die Rechte und die Interessen der betroffenen Personen zu wahren.

Art. 4

Die Anforderungen von Art. 4 E-VDSG gehen zu weit. Ein Bearbeitungsreglement wird abgelehnt. Sollte wider Erwarten am Bearbeitungsreglement festgehalten werden, gibt es keinen nachvollziehbaren Grund zur «regelmässigen» Überarbeitung desselben. Dieses muss dann überarbeitet werden, wenn es einen Anlass zur Aktualisierung gibt (Veränderung der Bearbeitungsmittel oder Formen).

Art. 6 Abs. 1 und 2

Die Pflicht, für den Verantwortlichen, die vertrags- und gesetzesmässige Bearbeitung durch den Auftragsbearbeiter «sicherzustellen» ist konzeptionell falsch. Richtig ist, dass der Verantwortliche sich gemäss Art. 9 Abs. 2 DSG vergewissern muss, dass die Datenbearbeitung korrekt erfolgt. Diese unverhältnismässige, nicht einzuhaltende und nicht vom Gesetzgeber vorgesehene Verschärfung der Pflicht des Verantwortlichen ist im Rahmen der Delegation an den Bundesrat als zu weit gehend zu betrachten.

➔ Formulierungsvorschläge für Art. 6 Abs. 1 2. Satz bzw.
Art. 6 Abs. 2 2. Satz E-VDSG:
Er vergewissert sich, dass die Daten vertrags- und gesetzesgemäss bearbeitet werden. / Andernfalls muss er sich auf dem vertraglichen Weg vergewissern, dass ein gleichwertiger Datenschutz gewährleistet wird.

Art. 9 Abs. 2 und Art. 10 Abs. 1

Auch diese Forderung an den Verantwortlichen geht zu weit, wenn er «sicherstellen» muss. Der Terminus «vergewissern» ist zu verwenden.

Art. 15 und 16

Diese Bestimmungen finden keine Grundlage im DSG und sind ersatzlos zu streichen. Die Berichtigung, Löschung, Vernichtung oder Einschränkung der Bearbeitung von Personendaten (Art. 16 E-VDSG) erfolgen zudem im Interesse der betroffenen Person. Diese müssen ja so oder so den Anforderungen des Gesetzes entsprechen. Wieso in solchen Situationen eine neue Informationspflicht im Interesse der betroffenen Person liegen soll, ist nicht klar. Im

Gegenteil: Mit einer solchen Information, sei sie auch noch so klar, wird die betroffene Person oft verunsichert oder zumindest auf einen Umstand aufmerksam gemacht, der dazu führt, dass Fragen aufgeworfen werden und Aufwand generiert wird, der dem Verantwortlichen nicht entschädigt wird. Das wird von der Wirtschaft in nachvollziehbarer Weise als unnötige und bürokratische Zusatzbelastung empfunden. Auf unnötige Informationen ist in den Beziehungen zwischen dem Datenbearbeiter und der betroffenen Person zu verzichten.

Art. 18

Die Aufbewahrungsfrist von 2 Jahren nach Beendigung der Datenbearbeitung entbehrt einer gesetzlichen Grundlage im DSG und ist als zu lange zu betrachten. Die Aufbewahrung hat höchstens bis zur Beendigung der entsprechenden Datenbearbeitung zu dauern, da danach keine Verletzung der Rechte der betroffenen Person mehr erfolgen kann. Für die Frage, ob jemand durch die Datenbearbeitung ein Schutzrecht der betroffenen Person verletzt hat, ist nicht die Datenschutz-Folgenabschätzung relevant, sondern die konkrete Datenbearbeitung und die entsprechenden Verzeichnisse und Reglemente des Verantwortlichen.

Art. 19 Abs. 1 Bst. b bis d

Diese Kriterien sind dem Gesetz nicht zu entnehmen. Der Bundesrat hat weder eine Delegation noch eine Ermächtigung erhalten, Art. 24 DSG zu ergänzen. Deshalb sind diese Buchstaben aus der Verordnung zu streichen.

Art. 19 Abs. 1 Bst. e

Bei der Entdeckung einer Verletzung der Datensicherheit ist es eben gerade nicht immer möglich, die Folgen und die allfälligen Risiken umgehend und abschliessend festzustellen. Deshalb muss beim Bst. e «*soweit möglich*» vorangestellt werden.

Art. 19 Abs. 3

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 Abs. 4 DSG hinausgeht.

Art. 19 Abs. 5

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wider Erwarten an einer Dokumentationspflicht festhalten, sind die 3 Jahre deutlich zu lang. Eine Aufbewahrungsdauer soll höchstens ein Jahr betragen.

Art. 20 Abs. 5

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 25 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wider Erwarten an einer Dokumentationspflicht festhalten, sind die 3 Jahre zu lang. Eine Aufbewahrungsdauer soll höchstens ein Jahr betragen.

Art. 22

Der Fristenlauf kann erst dann beginnen, wenn das Auskunftsgesuch formell korrekt eingereicht und inhaltlich klar ist. Solange das Gesuch entweder formell oder inhaltlich unklar ist,

kann die Frist nicht laufen. Dies muss im Art. 22 E-VDSG in aller Klarheit zum Ausdruck kommen.

Art. 23

Aufgrund der Einschränkungen, die gemäss Abs. 1 für die Kostenbeteiligung vom Bundesrat aufgestellt werden, steht der Betrag von CHF 300.00 in keiner vernünftigen Relation zum «unverhältnismässigen Aufwand». Bei Aufwendungen, die weit über CHF 1'000.00 gehen können, ist eine Kostenbeteiligung von nur gerade CHF 300.00 nicht angemessen. Natürlich hat der Verantwortliche die Kosten zu belegen. Aber es kann nicht sein, dass der Verantwortliche auf seinen Kosten sitzenbleibt und vom Kostenverursacher nur quasi ein symbolischer Betrag verlangt werden kann. Der Höchstbetrag ist deshalb anzuheben und sollte auf mindestens CHF 1'000.00 festgelegt werden.

Art. 24

Der Anspruch auf Datenportabilität bei der Datenherausgabe oder -übertragung, darf nicht ein absoluter sein. Dieser Anspruch darf nur bestehen, soweit die Bearbeitung von Personendaten in gängigen Formaten erfolgen kann bzw. erfolgt.

Art. 45 Abs. 1 und 2

Wenn die Kostenbeteiligung nach Art. 23 mit den Gebührengrundsätzen des EDÖB verglichen werden, dann muss von einer krassen Diskrepanz gesprochen werden. Der EDÖB erledigt eine Tätigkeit im Interesse der Bürger(innen) und der Volkswirtschaft Schweiz und es gibt keinen nachvollziehbaren Grund, weshalb die Person, welche Dienstleistungen von ihm in Anspruch nehmen muss, um sich datenschutzkonform zu verhalten, derart hohe Gebühren zu bezahlen hat. Weder kann es sein, dass die Gebühren nach Zeitaufwand berechnet werden (die Privatperson hat keinen Einfluss auf die Effizienz der Leistungserbringung durch den EDÖB), noch sind die Stundensätze von CHF 150.00 bis 350.00 angemessen. Diese Gebührenbestimmung stiftet die hilfesuchende Privatperson geradezu an, das Datenschutzrecht zu verletzen, da sie sich die Unterstützung durch den EDÖB nicht leisten kann. Die Gebührenordnung ist vollständig zu überdenken und auf ein vernünftiges Mass anzupassen. Hier wird dem Service-Public-Gedanken zu wenig Rechnung getragen. Es ist erforderlich, Maximalgebühren für Tätigkeiten festzulegen, welche der Einhaltung des Datenschutzrechts dienen (z.B. Art. 59 Abs. 1 Bst. c DSG, Konsultation aufgrund einer Datenschutz-Folgenabschätzung).

* *
*

Wir bitten Sie um Kenntnisnahme und danken für eine Berücksichtigung unserer Anliegen bestens.

Freundliche Grüsse

PRIVATE BILDUNG SCHWEIZ PBS

NR Dr. Gerhard Pfister
Präsident

Markus Fischer
Sekretär

pharmaSuisse
Schweizerischer Apothekerverband

pharmaSuisse, Stationsstrasse 12, 3097 Liebefeld

Bundesamt für Justiz
Direktionsbereich Öffentliches Recht
Fachbereich Rechtssetzungsprojekte
jonas.amstutz@bj.admin.ch

Bern-Liebefeld, 14. Oktober 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Frau Bundesrätin

Besten Dank für die Gelegenheit zur Stellungnahme in erwähnter Angelegenheit.

Die Wichtigkeit der Regelung der Details in der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) ist unbestritten. Die Verordnung trägt jedoch wenig zur Klärung von Detailfragen bei und überschreitet teilweise die vom revidierten Bundesgesetz über den Datenschutz (revDSG) festgelegten Grundlagen. pharmaSuisse lehnt die Verordnung im vorgelegten Entwurf ab und erachtet eine umfassende Überarbeitung als notwendig.

Dazu einige Punkte die hervorgehoben werden sollen:
- **Bearbeitungsreglement privater Personen (Art. 4)**: Art. 8 Abs. 3 revDSG bietet keine gesetzliche Grundlage für die Einführung eines Bearbeitungsreglement und überschreitet die gesetzlichen Delegationsvorgaben, da es sich hierbei nicht um Mindestanforderungen der Datensicherheit handelt. Eine Einführung eines Bearbeitungsreglement bedürfte einer eigenen gesetzlichen Grundlage.

- **Information bei der Bekanntgabe von Personendaten (Art. 15 und 16)**: Auch hier wird die gesetzliche Grundlage im revDSG (Art. 6 Abs 5 rev.DSG) deutlich zu weit ausgelegt und eine Verschärfung ohne gesetzliche Grundlage geschaffen. Aus dem revDSG ergibt sich eine Pflicht zur Information der Empfänger lediglich auf Verlangen einer betroffenen Person und nicht von sich aus. Die Verordnung geht insofern unnötigerweise weiter als das Gesetz.

- **Dokumentationspflichten**: Im revDSG wurden bewusst Dokumentationspflichten weggelassen, während andere im Gesetz ausführlich geregelt sind (unter anderem Art. 18. Abs. 5, Art. 19 Abs. 5 und Art. 20 Abs. 5). Diese entbehren ebenfalls einer gesetzlichen Grundlage, welche aufgrund ihres gemeinsam verursachten Aufwandes dringend notwendig wäre.

Ebenfalls ist den Unternehmen aufgrund des grossen zu erwartenden Aufwands eine angemessene Zeitspanne für die Umsetzung zu lassen. Insbesondere für kleinere Unternehmen, wie es Apotheken oft sind, ist die Umsetzung in kurzer Zeit nicht möglich. Deshalb ist für eine Einhaltung der Vorgaben eine Frist von einem Jahr notwendig.

Bei der Umsetzung an sich ist gerade für kleinere Unternehmen auf eine administrativ unkomplizierte Lösung zu achten, um den bereits jetzt grossen Dokumentationsaufwand nicht noch mehr ansteigen zu lassen.

Besten Dank für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

pharmaSuisse
Schweizerischer Apothekerverband

Samuel Dietrich
Jurist

Privacy Icons

Per E-Mail an:
fanny.matthey@bj.admin.ch
daniela.nueesch@bj.admin.ch

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Stellungnahme zum Vorentwurf Verordnung zum Datenschutzgesetz: Art. 13 Abs. 2 VE-VDSG ist ersatzlos zu streichen

Sehr geehrte Frau Matthey, sehr geehrte Frau Nüesch,
Sehr geehrte Damen und Herren,

Wir nehmen Bezug auf das Vernehmlassungsverfahren zum Vorentwurf für eine Verordnung zum Bundesgesetz über den Datenschutz (VE-VDSG) und beantragen namens des Vereins Privacy Icons, **Art. 13 Abs. 2 VE-VDSG ersatzlos zu streichen**.

Der Verein Privacy Icons ist ein Zusammenschluss renommierter Schweizer Unternehmen und Anwaltskanzleien mit dem Ziel, die Transparenz im Datenschutz zu erhöhen. Die von ihm herausgegebenen "Privacy Icons" sind Piktogramme, die bestimmte Aspekte der Datenbearbeitung für Kunden auf einen Blick sichtbar machen. Sie stehen allen Unternehmen zur kostenfreien Nutzung offen und werden bereits von verschiedenen bekannten Unternehmen genutzt, darunter Credit Suisse, Migros, SBB und Swisscom.

Der Verein Privacy Icons anerkennt, dass es wünschbar ist, wenn eingesetzte Piktogramme automatisiert verarbeitet werden können. Er lehnt aber eine verbindlich vorgeschriebene und nicht näher spezifizierte "Maschinenlesbarkeit", wie sie in Art. 13 Abs. 2 VE-VDSG vorgesehen ist, aus folgenden Gründen ab:

- **Die Bestimmung führt zu einem unerwünschten Ergebnis:** Piktogramme geben Orientierung und helfen, abstrakte datenschutzrechtliche Konzepte besser verständlich zu machen. Sie erhöhen die Transparenz und fördern damit ein zentrales Anliegen im Datenschutz. Es sollte Unternehmen einfach gemacht werden, Piktogramme zu nutzen und dadurch ihre Datenschutzhinweise leserfreundlicher zu gestalten. Die Anforderung einer "Maschinenlesbarkeit" in Art. 13 Abs. 2 VE-VDSG macht das Gegenteil. Sie erhöht die Hürden für eine Nutzung von Piktogrammen und wird dazu führen, dass weniger Unternehmen mit Hilfe von Piktogrammen die Verständlichkeit ihrer Datenschutzhinweise erhöhen. Sie führt somit zu einem rechtspolitisch unerwünschten Ergebnis.

- **Die Bestimmung verletzt rechtsstaatliche Grundsätze:** Art. 13 Abs. 2 VE-VDSG hat keine Grundlage im revidierten Datenschutzgesetz. Das revidierte Datenschutzgesetz wurde im Parlament ausführlich beraten und ist das Ergebnis eines politischen Kompromisses. Es ist nicht angängig, auf dem Verordnungsweg zusätzliche Anforderungen an die Informationspflicht einzuführen. Mit einer vorgeschriebenen Maschinenlesbarkeit von Piktogrammen überschreitet der Verordnungsgeber seine Rechtsetzungskompetenz.

- **Die Bestimmung schafft Rechtsunsicherheit:** Der Inhalt der Bestimmung ist unklar und auslegungsbedürftig. Für Herausgeber von Datenschutz-Piktogrammen und anwendende Unternehmen ist kaum abschätzbar, welche Anforderungen in der Praxis an eine "Maschinenlesbarkeit" gestellt werden. Diese Rechtsunsicherheit verstärkt den unerwünschten Effekt, dass die Bestimmung die Nutzung von Piktogrammen hindert, noch zusätzlich.

Privacy Icons

Art. 13 Abs. 2 VE-VDSG erschwert unnötigerweise die Verwendung von Piktogrammen, hat keine Grundlage im Gesetz und schafft Rechtsunsicherheit. Die Bestimmung ist ersatzlos zu streichen. Sollte die Bestimmung nicht vollumfänglich gestrichen werden, müsste der Verordnungstext zumindest dahingehend präzisiert werden, dass an die Maschinenlesbarkeit keine hohen Anforderungen gestellt werden und es z.B. genügt, wenn bei Bilddateien ein Erklärtext hinterlegt ist oder die Piktogramme als Schrift (Webfont) formatiert sind und sie somit von einem Computer verarbeitet werden können.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassungseingabe und stehen Ihnen bei Rückfragen gerne zur Verfügung.

Zürich, 2. September 2021

Juliette Hotz
Senior Counsel Data Governance
Swisscom (Schweiz) AG
Co-Präsidentin Privacy Icons

Dr. Matthias Glatthaar
Leiter Datenschutz & Digitalisierung
Migros Genossenschafts-Bund
Co-Präsident Privacy Icons

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail:
jonas.amstutz@bj.admin.ch

Bern, 1. September 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassungsverfahren

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) Stellung nehmen zu können. Gerne äussern wir uns dazu wie folgt:

1. Allgemeines

Das revidierte Bundesgesetz über den Datenschutz vom 25.09.2020 (revDSG) beinhaltet zahlreiche Delegationsnormen, auf die sich der vorliegende E-VDSG stützt (siehe Ingress E-VDSG). Zudem konkretisiert der E-VDSG verschiedene Bestimmungen des revDSG.

Insgesamt entsteht der Eindruck einer Verordnung, die (zu) wenig Klarheit für die Umsetzung durch die Verantwortlichen schafft. Einerseits liegt es darin, dass überholte Begriffe und Bestimmungen der bisherigen Verordnung einfach übernommen werden. Andererseits bringen die neuen Bestimmungen nicht die notwendige Detaillierung für die Umsetzung des an sich schon komplexen revDSG.

Die Verantwortlichen – private Personen wie auch Bundesorgane – werden Mühe haben, verschiedene dieser Bestimmungen angemessen umzusetzen.

Das Konzept der E-VDSG und einzelne Bestimmungen sollten deshalb im Hinblick auf eine wirkungsvolle Umsetzung des Datenschutzes grundsätzlich überprüft werden.

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, CH-3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

2. Einzelne Bestimmungen

a. Art. 1 bis 4 E-VDSG (Datensicherheit)

Die Art. 1 bis 4 E-VDSG konkretisieren die Anforderungen an die Datensicherheit (Art. 8 revDSG). Dabei verlangt Art. 8 Abs. 3 revDSG, dass der Bundesrat Mindestanforderungen an die Datensicherheit erlässt.

Der E-VDSG verpasst es, diese Mindestanforderungen in einer Form zu konkretisieren, die auch in Bezug auf die strafbewehrte Unterlassung der Umsetzung der Mindestanforderungen (Art. 61 Abs. 1 Bst. c revDSG) objektive Tatbestandsmerkmale erkennen lassen würde. In Bezug auf die Datensicherheit ist in der Informationsbearbeitung heute ein Standard erreicht, der klar nach der Beurteilung des Schutzbedarfs und der Risiken die entsprechenden Sicherheitsmassnahmen vorschlägt und einteilt (Grundschutz, hoher Schutz, sehr hoher Schutz). Der Bund hat soeben mit der Verabschiedung des Bundesgesetzes über die Informationssicherheit (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020) gezeigt, wie die heutigen Anforderungen auch gesetzestechnisch umgesetzt werden können.

Der E-VDSG hält dagegen am veralteten Konzept der bisherigen Verordnung fest und ergänzt diese mit Begriffen aus dem europäischen Recht, ohne aber Art. 8 revDSG für die Praxis zu konkretisieren.

Der Abschnitt 1 (Datensicherheit) ist aus unserer Sicht konzeptionell grundsätzlich zu überarbeiten.

b. Art. 1 E-VDSG

Art. 1 Abs. 1 E-VDSG schreibt eine Beurteilung der Angemessenheit von Massnahmen nach den Kriterien Zweck, Art, Umfang und Umstände der Datenbearbeitung, Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen, Stand der Technik und Implementierungskosten vor.

Hier wird im Wesentlichen Art. 32 DSGVO rezipiert, ohne aber das in diesem Artikel formulierte Ziel in den Vordergrund zu stellen: «ein dem Risiko angemessenes Schutzniveau zu gewährleisten».

Mitunter bedeutet dies, dass die Schutzziele, der Schutzbedarf und die Risiken zuerst zu beurteilen sind.

Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt, wie dies auch die Erläuterungen erwähnen (S. 15) und werden in Art. 2 E-VDSG ausführlich aufgezählt (siehe nachfolgend Art. 2 E-VDSG). Der Schutzbedarf ergibt sich aus der Art der Daten (Personendaten, besonders schützenswerte Personendaten) und der Datenbearbeitung selbst (z.B. Profiling). Erst dann erfolgt die Risikobeurteilung, wie dies auch die Datenschutz-Folgenabschätzung vorsieht (Art. 22 revDSG).

Die Kriterien «Zweck, Art, Umfang und Umstände der Datenbearbeitung» beziehen sich somit auf die Schutzbedarfsfeststellung (welche bereits eine erste grobe Einschätzung des möglichen Schadensausmasses enthält), die Kriterien «Eintrittswahrscheinlichkeit und potenzielle Auswirkungen für die betroffenen Personen» auf die Risikobeurteilung.

Wenn es um die Beurteilung der Angemessenheit der Massnahmen geht, sind die Kriterien «Stand der Technik und Implementierungskosten» einschlägig. Sie sagen aber nur indirekt etwas über die Angemessenheit einer Massnahme aus, da in Bezug auf die Angemessenheit von Massnahmen in erster Linie zu beurteilen ist, ob eine Massnahme zu treffen ist und konkret welche dem Risiko mit der nötigen Effektivität begegnet. Dies ist im erwähnten ISG so angelegt, aber auch in Art. 32 DSGVO, der hier zitiert wird (Erläuterungen, S. 15).

Art. 1 Abs. 1 E-VDSG ist deshalb konzeptionell grundsätzlich zu überarbeiten.

Art. 1 Abs. 2 E-VDSG verlangt, dass die Massnahmen über die gesamte Bearbeitungszeit in angemessenen Abständen zu überprüfen sind. Diese Formulierung greift zu kurz. In erster Linie ist die Risikobeurteilung laufend zu überprüfen, woraus sich die Massnahmen und deren Angemessenheit ergeben und somit die allfällige Anpassung von Massnahmen.

Die Formulierung ist zu korrigieren.

c. Art. 2 E-VDSG

Die Aufzählung der Schutzziele wurde aus der geltenden Verordnung übernommen und mit Bestimmungen aus der DSGVO ergänzt.

Die Schutzziele sind bereits in Art. 5 Abs. 1 Bst. h revDSG angelegt und lassen sich in die in der Informatiksicherheit üblichen Schutzziele zusammenfassen: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit (so auch Erläuterungen, S. 15). Er erscheint als angezeigt, dies entsprechend klar zum Ausdruck zu bringen (vgl. in diesem Sinne Art. 6 Abs. 2 des Informationssicherheitsgesetzes vom 18.12.2020).

Die in Art. 2 aufgeführten Vorgaben stellen keine eigenständigen Schutzziele dar, sondern Anforderungen an die Massnahmen, welche zur Erreichung der Schutzziele zu treffen sind (so stellt etwa die Zugriffskontrolle kein Schutzziel dar, sondern eine Anforderung zur Gewährleistung der Vertraulichkeit im Rahmen des Verhältnismässigkeitsprinzips).

Zudem ist der Einleitungssatz von Art. 2 E-VDSG missverständlich. Schutzziele sind Zielvorgaben. Die Massnahmen müssen angemessen sein in Bezug auf die in der Risikobeurteilung festgestellten Risiken und nicht in Bezug auf die Schutzziele.

d. Art. 3 E-VDSG

Art. 3 E-VDSG sieht insbesondere für Bundesorgane eine ausführliche Protokollierung der Datenbearbeitungen vor.

Die Protokollierung hat zum Zweck, dass in Situationen, wo ein unberechtigtes Bearbeiten von Personendaten nicht zum vornherein technisch ausgeschlossen werden kann, im Nachhinein mittels Auswertung eines Protokolls ein unberechtigtes Bearbeiten festgestellt (und dann unter Umständen sanktioniert) werden kann. Mithin ergibt sich die Protokollierung aus der Risikobeurteilung und der Massnahmenplanung. Sie muss also ein geeignetes Mittel mit Blick auf ein konkretes Risiko sein, das mittels Protokollierung wirksam reduziert werden kann; dass ein *irgendwie* geartetes Risiko verbleibt, reicht nicht (es fehlt dann an der Verhältnismässigkeit der neuen Datenbearbeitung). Soweit ersichtlich ist der Hauptanwendungsfall der, dass aus betrieblichen Gründen zu umfassende Berechtigungen implementiert werden müssen, weil nicht zum Vorherein bekannt ist, auf welche konkreten Daten

der/die Berechtigte bei der Aufgabenerfüllung Zugang haben muss (z.B. im Schengen-Informationssystem). Hier kann die organisatorische Massnahme eines Dienstbefehls wirksam verstärkt werden, wenn die tatsächlichen Datenabrufe protokolliert und stichprobenweise überprüft werden. Die Pflicht zur Protokollierung als kompensierende Massnahme ist deshalb nur für jene Fälle zu statuieren, in denen sie das festgestellte Risiko auch tatsächlich adressiert.

Für die Bundesorgane soll die Protokollierung für das Bearbeiten sämtlicher Personendaten gelten (Art. 3 Abs. 2 E-VDSG). Hier wird weit über das Ziel hinausgeschossen. Die Protokollierung stellt selbst eine Beschaffung von Personendaten dar, die dem Grundsatz der Verhältnismässigkeit genügen muss. Zwar erlaubt Art. 57*l* Bst. b Ziff. 4 RVOG die Aufzeichnung von Randdaten zum Nachvollzug des Zugriffs auf Datensammlungen, aber eben nur insoweit, als die Aufzeichnung verhältnismässig ist. Dass selbst bei einfachen Personendaten und selbst bei restriktiven Berechtigungen jeder Lesezugriff protokolliert werden soll, geht klar über diese Anforderung hinaus. Die Bundesorgane sind deshalb in Absatz 1 aufzunehmen und auf Absatz 2 ist zu verzichten.

In Art. 3 Abs. 3 E-VDSG sollte vor «die Identität der Empfängerin oder des Empfängers» das Wort «gegebenenfalls» eingefügt werden, da es sich nicht bei jeder protokollierten Bearbeitung um eine Bekanntgabe handelt.

Gemäss Art. 3 Abs. 4 E-VDSG sind die Protokolle während zweier Jahre aufzubewahren und dürfen nur zur Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten verwendet werden. Dabei ist nicht in jedem Fall eine personenbezogene Auswertung erforderlich. Für die Bundesorgane legen die Art. 57*m* ff. RVOG und Art. 8 ff. der zugehörigen Ausführungsverordnung fest, wie die Auswertungen erfolgen dürfen, wobei ggf. auch ein gestaffeltes Vorgehen angezeigt ist (vgl. BGE 143 II 443). Der letzte Satz ist deshalb im Sinne «dürfen nur zu diesem Zweck und nur soweit erforderlich personenbezogen verwendet werden» zu ergänzen.

e. Art. 4 E-VDSG

Die Erstellung eines Bearbeitungsreglements wird für private Verantwortliche und deren Auftragsbearbeiter vorgesehen, die (1) umfangreich besonders schützenswerte Personendaten bearbeiten oder (2) ein Profiling mit hohem Risiko durchführen (Art. 4 Abs. 1 E-VDSG). Diese Eingrenzung erscheint willkürlich und deckt bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen ab.

Hier ist es angezeigt, die Voraussetzungen für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG). Im Rahmen der Datenschutz-Folgenabschätzung werden zudem zahlreiche Dokumente erstellt (Art. 22 Abs. 3 revDSG), die Teil des Bearbeitungsreglements sein können.

Art. 4 Abs. 2 E-VDSG enthält Mindestangaben für das Datenbearbeitungsreglement. Auch hier wird kein Konnex zu den Standards in der Informatik gemacht, in dem auf diese verwiesen würde. Dann würde es genügen, auf die spezifischen datenschutzrechtlichen Vorgaben hinzuweisen (Bst. h, j).

Art. 4 Abs. 3 E-VDSG erscheint praxisfern. Die Datenschutzberaterin oder der Datenschutzberater ist die Fachperson bei einem Verantwortlichen und ein Bearbeitungsreglement wird zusammen mit ihr/ihm erstellt und nicht «der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung» gestellt. Es gehört zu den Aufgaben der Datenschutzberaterin oder des Datenschutzberaters, bei der Anwendung der Datenschutzvorschriften mitzuwirken (Art. 10 Abs. 2 Bst. b revDSG). Zudem hat die Datenschutzberaterin oder der Datenschutzberater über die erforderlichen Fachkenntnisse zu verfügen (Art. 10 Abs. 3 Bst. c revDSG), weshalb die Formulierung, das Bearbeitungsreglement sei ihr oder ihm «in verständlicher Form» zur Verfügung zu stellen, offensichtlich eine Abwertung seiner Fachkompetenzen impliziert.

Art. 4 Abs. 3 E-VDSG ist ersatzlos zu streichen.

f. Art. 5 E-VDSG

Grundsätzlich kann auf unsere Ausführungen zu Art. 4 E-VDSG verwiesen werden.

g. Art. 7 E-VDSG

Auch die Datenschutzberaterin oder der Datenschutzberater des Bundesorgans hat bei der Anwendung der Datenschutzvorschriften mitzuwirken (vgl. unten Art. 28 E-VDSG). Es widerspricht dem präventiven und risikoorientierten Ansatz des revDSG, wenn die Datenschutzberaterin oder der Datenschutzberater lediglich nachträglich über den Abschluss eines Outsourcingvertrags oder bei einer Funktionsübertragung informiert werden soll. Zu den Aufgaben einer Datenschutzberaterin oder eines Datenschutzberaters gehört die Involvierung in solche Geschäfte. Die ist eine Kernaufgabe der Beraterin oder des Beraters («Mitwirkung bei der Anwendung der Datenschutzvorschriften»). Die Datenschutzberaterin oder der Datenschutzberater ist rechtzeitig zu informieren, wie dies korrekterweise bei Datenbearbeitungsprojekten vorgesehen ist (Art. 31 E-VDSG).

Art. 7 E-VDSG ist ersatzlos zu streichen.

h. Art. 8 E-VDSG

Bei den Formulierungen in Art. 8 E-VDSG fällt auf, dass der EDÖB konsultiert wird (formell), und die Beurteilungen von internationalen Organisationen oder ausländischen Behörden berücksichtigt werden können (materiell). Es ist klar zu formulieren, dass auch die Stellungnahmen des EDÖB materiell zu berücksichtigen sind, zumal sich die Erläuterungen hierzu nicht äussern (Erläuterungen, S. 27).

i. Art. 9 Abs. 3 E-VDSG

Gemäss Art. 16 Abs. 2 Bst. b und c revDSG sind Datenschutzklauseln und spezifische Garantien dem EDÖB vorgängig mitzuteilen. Der Einleitungssatz von Art. 9 Abs. 3 E-VDSG suggeriert, dass es einen Sachverhalt geben könnte, in der auch die Nicht-Mitteilung zu einer rechtskonformen Bekanntgabe ins Ausland führen würde.

Die Formulierung ist anzupassen.

j. Art. 19 E-VDSG

Art. 24 Abs. 1 revDSG sieht eine Meldung von Verletzungen der Datensicherheit nur in Fällen vor, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Art. 24 Abs. 2 revDSG präzisiert den Inhalt der Meldung und nennt die Voraussetzungen für die Information der betroffenen Personen (Art. 24 Abs. 4 und 5 revDSG).

Art. 24 revDSG ist eine (bewusst) abweichende Bestimmung von Art. 33 DSGVO. Dennoch werden in Art. 19 E-VDSG mehrheitlich die Bestimmungen von Art. 33 DSGVO rezipiert. Dies ist einzig für Verantwortliche dienlich, die auch der DSGVO unterliegen. Für die Mehrheit der Verantwortlichen ist dies aber nicht der Fall und Art. 19 E-VDSG bringt unnötige Zusatzbestimmungen, vielfach eingeschränkt mit der Bemerkung «wenn möglich». Dies ist dem Institut der Meldepflicht wenig dienlich: Es will ja in erster Linie, dass die Aufsichtsbehörde rasch informiert wird, allenfalls auch die betroffenen Personen, und dass Massnahmen zum Schutz der Personendaten umgehend getroffen werden.

Art. 24 revDSG braucht die in Art. 19 E-VDSG enthaltene Konkretisierung nicht.

k. Art. 20 E-VDSG

Art. 25 revDSG und Art. 26 revDSG regeln das Auskunftsrecht und dessen Einschränkungen ausführlich. Art. 20 E-VDSG bringt hierzu einige Konkretisierungen, die aber über das Notwendige hinausgehen.

Art. 20 Abs. 3 E-VDSG hält fest, dass die Auskunft für die betroffene Person verständlich sein muss. Dies ist irreführend. Der Inhalt der Auskunft ist in Art. 25 Abs. 2 revDSG definiert. Daraus ergeben sich der Umfang und der Zweck der Auskunft. Dies misst sich nach objektiven Kriterien. Das Abstellen auf die individuell um Auskunft ersuchende Person würde für den Verantwortlichen bedeuten, dass er mehr Angaben zu dieser Person bearbeiten müsste und das Auskunftsrecht nicht mehr als selbstverständlicher Standard des Datenschutzrechts in die Prozesse des Verantwortlichen integriert werden könnte.

Art. 20 Abs. 3 E-VDSG ist ersatzlos zu streichen.

Art. 20 Abs. 4 E-VDSG enthält unnötigerweise die Auflage an die Verantwortlichen, «die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen». Dies ergibt sich bereits aus Art. 8 revDSG und den Bestimmungen des 1. Kapitels der E-VDSG.

Diese Erwähnung ist in Art. 20 Abs. 4 E-VDSG zu streichen.

Art. 26 Abs. 4 revDSG sieht vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies ist ausreichend für die betroffene Person, um ihren Auskunftsanspruch allenfalls gerichtlich geltend zu machen. Die Auflage an den Verantwortlichen in Art. 20 Abs. 5 E-VDSG, die Einschränkung des Auskunftsrechts zu dokumentieren und diese Dokumentation mindestens drei Jahre aufzubewahren, bringt einen Mehraufwand, ohne irgendwelche Auswirkungen im Hinblick auf die Geltendmachung oder die Durchsetzung des Auskunftsrechts durch die betroffene Person.

Art. 20 Abs. 5 E-VDSG ist ersatzlos zu streichen.

l. Art. 21 E-VDSG

Art. 21 Abs. 1 E-VDSG sieht vor, dass ein Verantwortlicher, der für die Behandlung des Begehrens nicht zuständig, dieses an den zuständigen Verantwortlichen weiterleitet. Dieser verwaltungsrechtliche Grundsatz gilt für die Bundesorgane auch ohne Erwähnung in diesem Zusammenhang. Im öffentlich-rechtlichen Bereich ergibt er sich aus dem hoheitlichen Verhältnis der Bürgerinnen und Bürger zum Staat. Im privatrechtlichen Verhältnis legen die Parteien ihre Rechte und Pflichten aber autonom fest. Die gleiche Auflage auch dem privatrechtlichen Verantwortlichen zu machen, ist unverhältnismässig. Sie führt zu einem Aufwand für den privatrechtlichen Verantwortlichen, den «zuständigen» Verantwortlichen ausfindig zu machen, ohne dass dadurch die Rechte der betroffenen Personen gestärkt würden.

Art. 21 Abs. 1, 2. Satz E-VDSG ist ersatzlos zu streichen.

m. Art. 24 E-VDSG

Art. 24 E-VDSG beinhaltet eine Konkretisierung von Art. 28 revDSG, indem er sich auf die sinngemässe Anwendung von Bestimmungen zum Auskunftsrecht verweist. Dies wird dem neuen Rechtsinstitut der «Datenportabilität» nicht gerecht und verkennt den durchaus vorhandenen Bedarf einer Konkretisierung der gesetzlichen Bestimmung (beispielsweise in Bezug auf die «gängigen elektronischen Formate» oder den «unverhältnismässigen Aufwand» bei der direkten Übertragung von einem Verantwortlichen zu einem anderen). Zudem wäre auch in Bezug auf die Ausnahmen der Kostenlosigkeit eine andere Regelung als beim Auskunftsrecht denkbar, da hier nicht der Persönlichkeitsschutz, sondern der wirtschaftliche Wert der Daten im Vordergrund steht.

Art. 24 E-VDSG ist vollständig zu überarbeiten.

n. Art. 25 E-VDSG

Art. 25 E-VDSG hält fest, welche Aufgaben die Datenschutzberaterin oder der Datenschutzberater wahrnehmen muss. Es wird dabei kein Bezug genommen zu Art. 10 Abs. 2 revDSG, der namentlich zwei Aufgaben aufzählt: die Schulung und Beratung sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Diese gesetzlichen Aufgaben sind umfassend, weshalb die Aufgaben in Art. 25 Abs. 1 Bst. a und b E-VDSG nicht die Aufgaben sind, die er oder sie wahrnehmen muss, sondern lediglich eine Konkretisierung der bereits in Art. 10 Abs. 2 revDSG festgehaltenen Aufgaben. Die Formulierung in Art. 25 Abs. 1 E-VDSG ist missverständlich und zu korrigieren.

o. Art. 26 E-VDSG

In Anwendung von Art. 12 Abs. 5 revDSG sieht Art. 26 E-VDSG vor, dass Verantwortliche mit weniger als 250 Mitarbeitenden nur ein Verzeichnis der Bearbeitungstätigkeiten führen müssen, wenn (1) umfangreich besonders schützenswerte Personendaten bearbeitet werden oder (2) ein Profiling mit hohem Risiko durchgeführt wird. Wie bei Art. 4 Abs. 1 E-VDSG ist zu erwähnen, dass diese Eingrenzung bei Weitem nicht die für die Persönlichkeitsrechte kritischen Datenbearbeitungen abdeckt. Auch hier ist es angezeigt, die Voraussetzungen

für die Datenschutz-Folgenabschätzung zu übernehmen (Bearbeitung beinhaltet ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen; Art. 22 Abs. 1 revDSG).

p. Art. 28 E-VDSG

Art. 28 E-VDSG legt die Aufgaben der Datenschutzberaterin oder -beraters der Bundesorgane fest. In der Aufzählung von Art. 28 Abs. 2 E-VDSG fällt auf, dass die in Art. 10 Abs. 2 Bst. b revDSG festgelegte Aufgabe – die Mitwirkung bei der Anwendung der Datenschutzvorschriften – nicht erwähnt wird, sondern nur die Schulung und Beratung (Art. 10 Abs. 2 Bst. a revDSG). Wir gehen davon aus, dass es sich hier um ein Versehen handelt, ist doch die Mitwirkung bei der Anwendung der Datenschutzvorschriften eine Kernaufgabe von Datenschutzberaterinnen und -berater. Diese Aufgabe ist in Art. 28 Abs. 2 E-VDSG zu ergänzen.

q. Art. 36 E-VDSG

Die Bestimmung ist überflüssig, weil sich diese Präzisierung bereits aus Art. 39 revDSG klar ergibt.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim

Dachverband
gemeinnütziger
Stiftungen
der Schweiz

Dufourstrasse 49
CH-4052 Basel
Schweiz

Telefon +41 61 272 10 80
Telefax +41 61 272 10 81
www.profonds.org

per Mail: danielle.schneider@bj.admin.ch / jonas.amstutz@bj.admin.ch

Frau Bundesrätin
Karin Keller Sutter
Eidgenössisches Justiz- und Polizeidepartement
CH-3003 Bern

Basel, 6. Oktober 2021

Vernehmlassung zum Vorentwurf zur Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin

proFonds, Dachverband gemeinnütziger Stiftungen der Schweiz, vertritt gesamtschweizerisch die Interessen *gemeinnütziger Stiftungen und Vereine* aller Tätigkeits- und Finanzierungsformen. Dem Gemeinnützigkeitswesen kommt in der Schweiz eine sehr grosse Bedeutung zu. Die über 13'000 gemeinnützigen Stiftungen und die zahlreichen gemeinnützigen Vereine üben im Interesse und zum Wohl der Allgemeinheit wichtige Funktionen aus, etwa in den Bereichen Soziales, Gesundheitswesen, Forschung und Wissenschaft, Bildung und Erziehung, Jugendförderung, Kunst, Kultur, Entwicklungszusammenarbeit etc.

Gerne machen wir von der Möglichkeit Gebrauch, zum Vorentwurf der Verordnung zum Bundesgesetz über den Datenschutz (VE-VDSG) eine Vernehmlassung einzureichen.

Vorbemerkung

Zahlreiche gemeinnützige Stiftungen und Vereine werden vom totalrevidierten Datenschutzgesetz und entsprechend von der Verordnung betroffen sein. Im Vordergrund stehen namentlich Aktivitäten im Zusammenhang mit dem Fundraising (Spenderdaten) sowie die Förderung (Daten von Destinatären) und – für Vereine – den Mitgliederdaten. In diesen Bereichen werden Personendaten bearbeitet.

Beim Gros der gemeinnützigen Stiftungen und Vereine handelt es sich um kleinere und mittlere Organisationen ohne nennenswerte Personalressourcen. Nach wie vor ist die Ehrenamtlichkeit, d. h. unentgeltliches Engagement, weit verbreitet, namentlich in den Leitungsgremien (Stiftungsrat und Vereinsvorstand). Der Grossteil der gemeinnützigen Stiftungen und Vereine verfügt auch über sehr begrenzte finanzielle Mittel. Deshalb ist es erforderlich, dass die Umsetzung des Datenschutzgesetzes auch für solche Organisationen machbar bleibt.

Zu den einzelnen Bestimmungen in dem VE-VDSG (Auswahl)

Zu Art. 1

Die Angemessenheit der Massnahme ist nicht nur nach den Implementierungskosten (Art. 1 lit. d VE-VDSG), sondern auch nach dem sonstigen Implementierungsaufwand zu beurteilen. Hierzu sind sämtliche Aufwendungen zu berücksichtigen, wie auch personelle Aufwendungen, deren Kosten nicht ausschliesslich der Implementierung hinzugerechnet werden können.

Die Ausführungen im erläuternden Bericht sind widersprüchlich, wenn ausgeführt wird, dass der Verantwortliche oder Auftragsbearbeiter sich nicht von der Pflicht einer angemessenen Datensicherheit mit dem Verweis auf übermässige Kosten befreien könne, die Implementierungskosten aber zu berücksichtigen sind. Offenkundig sind die Kosten als Kriterium der Angemessenheit heranzuziehen.

Gerade bei kleineren und mittleren Stiftungen und Vereinen ist es existenziell, dass sämtliche Aufwendungen, die im Zusammenhang mit der Sicherstellung der Datensicherheit getätigt werden, für die Beurteilung der Angemessenheit der Datensicherheit berücksichtigt werden. Ziel des Heranziehens des Kostenaspekts ist es ja nicht, sich den datenschutzrechtlichen Anforderungen zu entziehen, sondern diese für kleinere und mittlere Organisationen auch tatsächlich umsetzbar zu machen. Hier ist also behördliches Augenmass gefragt. Die Bestimmung ist zu präzisieren.

Zu Art. 4

Das Erstellen eines Bearbeitungsreglements, wenn umfangreiche besonders schützenswerte Daten bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird, ist gesetzlich nicht vorgesehen. Für diese zusätzliche, nicht unbedeutende Pflicht fehlt es somit an einer gesetzlichen Grundlage.

Eine Vielzahl gemeinnütziger Stiftungen und Vereine bearbeiten besonders schützenswerte Daten, sei dies namentlich im Sozial-, Gesundheits- oder im Wissenschaftsbereich. Es ist nicht einzusehen, weshalb diese Organisationen nun durch die Hintertür mit einer Anmeldepflicht einer Datensammlung konfrontiert werden, obwohl der Gesetzgeber diese Anmeldepflicht durch das Führen eines Bearbeitungsverzeichnisses ersetzt hat. Der Umstand, dass Art. 11a DSG keinen Einzug in das neue DSG (nDSG) gefunden hat, ist ja auch dem erläuternden Bericht zu entnehmen. Umso unverständlicher ist der vorliegende Versuch, dies wiedereinzuführen. Die Bestimmung ist daher zu streichen.

Zu Art. 6

Art. 6 Abs. 1 VE-VDSG sieht vor, dass der Verantwortliche bei einer Datenbearbeitung durch einen Auftragsbearbeiter sicherstellen muss, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.

Dazu muss es genügen, wenn der Verantwortliche dem Auftragsbearbeiter die gesetzlichen Pflichten vertraglich überbindet und ihn damit zu einer gesetzeskonformen Datenbearbeitung anhält.

Gerade kleinere und mittlere Stiftungen, Vereine und NPO geben gewisse Datenbearbeitungen extern (bspw. im Rahmen des Fundraising). Diese haben in aller Regel weder die Möglichkeit noch die Ressourcen eine umfassende Kontrolle vorzunehmen. Daher ist vorzusehen, dass der Verantwortliche die Auftragsbearbeitung vertraglich so auszugestalten hat, dass sie gesetzeskonform ist.

Zu Art. 13

Vorneweg ist festzuhalten, dass die Informationspflicht nach Art. 19 nDSG dem Verantwortlichen auferlegt ist. Auf welcher Grundlage der VE-VDSG nun auch für den Auftragsbearbeiter eine solche Pflicht begründen will, ist nicht ersichtlich. Es fehlt an einer gesetzlichen Grundlage. Die Bestimmung ist entsprechend zu korrigieren, d.h. die Pflicht für den Auftragsbearbeiter zu streichen.

Gemäss dem erläuternden Bericht muss die Information stets auf der ersten Kommunikationsstufe erfolgen. Was damit genau gemeint ist, ist dem Bericht nicht zu entnehmen. Reicht der Verweis auf der Entry Page auf eine Datenschutzerklärung?

Auch ist nicht klar, was damit gemeint ist, dass es "eine gute Praxis wäre", wenn alle Informationen auf "einen Blick verfügbar" wären. Ist das eine gestalterische Vorgabe? Muss ein Inhaltsverzeichnis erstellt werden?

Die Ausführungen im erläuternden Bericht sind insbesondere dann gänzlich unklar, wenn der Verantwortliche nicht im digitalen Bereich seiner Informationspflicht nachzukommen hat. Muss bei einer Anfrage am Telefon einer gemeinnützigen Organisation die u.U. mehrseitige Datenschutzerklärung vorgelesen werden? Muss im Rahmen des Fundraising bei jedem ersten Briefkontakt die Datenschutzerklärung mitgesendet werden? Dies wäre klar unverhältnismässig!

Leider verpasst es der VE-VDSG und der erläuternde Bericht, hier Klarheit zu schaffen. proFonds vertritt die Ansicht, dass es genügen muss, wenn der Datenbearbeiter über seine Website seiner Informationspflicht nachkommt. Es ist zumutbar, dass sich Betroffene (gegebenenfalls nach einem ausdrücklichen Verweis auf die Website) dort informieren.

Die Regelung in Art. 13 VE-VDSG ist nach dem Gesagten unklar. Durch die unpräzise Formulierung schafft diese Bestimmung Rechtsunsicherheiten. Es wäre zu wünschen, dass sich der Verordnungsgeber den praktischen Bedürfnissen der Verantwortlichen und der Betroffenen annimmt und einen praktikablen Umgang vorsieht.

Zu Art. 15

Vorneweg ist festzuhalten, dass auch in Art. 15 VE-VDSG neben den Verantwortlichen wiederum die Auftragsbearbeiter verpflichtet werden sollen. Diese haben aber keine Informationspflicht.

Des Weiteren fehlt es auch dieser weitergehenden Pflicht an einer gesetzlichen Grundlage. Sie ist auch nicht umsetzbar. Der Verantwortliche wird ohne unverhältnismässigen Aufwand nicht ununterbrochen über die Aktualität, Zuverlässigkeit und Vollständigkeit informieren können. Diese zusätzliche Regelung ist auch nicht notwendig.

Im Gegenteil: Es gelten die Grundsätze nach Art. 6 nDSG. Gemäss Art. 6 Abs. 5 nDSG muss sich der Datenbearbeiter über die Richtigkeit der von ihm bearbeiteten Daten vergewissern. Dies umfasst bereits eine Prüfung der Aktualität und Vollständigkeit und mit der Sicherstellung der Richtigkeit der Daten sind diese auch zuverlässig. Die Interessen des Betroffenen sind damit ausreichend geschützt. Er darf gestützt auf Art. 6 nDSG davon ausgehen, dass die über ihn erhobenen Daten korrekt sind. Eine zusätzliche Informationspflicht geht über die gesetzlichen Anforderungen hinaus und plustert den ohnehin reichhaltigen Pflichtenkatalog nur unnötig auf.

Art. 15 VE-VDSG ist aus diesem Grund ersatzlos zu streichen.

Zu Art. 16

Art. 16 VE-VDSG entspricht Art. 19 lit. b VE-DSG. Dieser wurde nach der Vernehmlassung gestrichen. Entsprechend kann es nicht sein, dass diese Pflicht nun auf Verordnungsebene wiedereingeführt wird. Der Wille des Gesetzgebers ist zu respektieren und Art. 16 VE-VDSG ist ersatzlos zu streichen.

Zu Art. 18

Die Datenschutz-Folgenabschätzung sollte mit Blick auf die strenge bundesverwaltungsgerichtliche Auslegung des Begriffs der Schriftlichkeit gemäss Art. 14 OR (BVerwGer A-3548/2018 vom 19. März 201, E. 4.8) nicht "schriftlich" festgehalten werden. Vielmehr sollte der Nachweis durch Text genügen.

Zu Art. 19

Art. 19 Abs. 5 VE-VDSG stipuliert die Dokumentationspflicht von Datenschutzverletzungen. Die Anforderung, wonach "alle mit den Vorfällen zusammenhängenden Tatsachen" dokumentiert werden müssen, ist gerade für mittlere und kleinere Stiftungen, Vereine und NPO nicht umsetzbar. Diese Pflicht geht viel zu weit und generiert einen unverhältnismässigen Aufwand.

Des Weiteren ist die Aufbewahrungsfrist – im Gleichlauf zu Art. 18 VE-VDSG – auf zwei Jahre zu reduzieren.

Zu Art. 20

Die Erteilung der angeforderten Auskunft sollte in irgendeiner Textform (also auch digital) möglich sein. Das Schriftlichkeitserfordernis geht zu weit und ist auch nicht praktikabel.

Für die Frage, ob die Auskunft für die betroffene Person verständlich ist (Art. 20 Abs. 3 VE-VDSG), ist ein objektivierter Massstab heranzuziehen. Persönliches Unvermögen der betroffenen Person darf nicht zur Annahme einer Pflichtverletzung des Verantwortlichen führen. Des Weiteren ist auch hier die Aufbewahrungsfrist – im Gleichlauf zu Art. 18 VE-VDSG – auf zwei Jahre zu reduzieren.

Art. Art. 26

proFonds begrüsst ausdrücklich die Regelung in Art. 26 VE-VDSG, wonach eine privatrechtliche Organisation, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigt, von der Pflicht befreit ist, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, es sei denn, es werden umfangreich besonders schützenswerte Personendaten bearbeitet oder es wird ein Profiling mit hohem Risiko durchgeführt.

Stiftungen unterstehen der Revisionspflicht (Art. 83b ZGB). In Übereinstimmung mit Art. 727 OR, wonach eine ordentliche Revision vorzunehmen ist, wenn in zwei aufeinander folgenden Geschäftsjahren 250 Vollzeitstellen im Jahresdurchschnitt überschritten werden, sollte in Art. 26 VE-VDSG ebenfalls auf 250 Vollzeitstellen im Jahresdurchschnitt abgestellt werden. Damit sind Stiftungen und Vereine, die aufgrund ihrer Mitarbeiteranzahl zur ordentlichen Revision verpflichtet sind, auch zur Führung eines Verarbeitungsverzeichnisses verpflichtet. Damit wird eine gesetzliche Kohärenz geschaffen.

Zusammenfassende Betrachtung

Es ist Sache der VDSG, die datenschutzrechtlichen Anforderungen gemäss dem neuen Gesetz so zu präzisieren, dass sie einerseits praktikabel und umsetzbar sind, andererseits aber auch dem gesetzgeberischen Willen entsprechen. Diesen Spagat schafft die VDSG an zahlreichen Stellen nicht.

****

Wir danken Ihnen für die aufmerksame Prüfung unserer Standpunkte. Wir hoffen, dass unsere Vorschläge bei der weiteren Bearbeitung der Vorlage Berücksichtigung finden. Für eine Vertiefung spezifischer Fragen steht proFonds jederzeit gerne zur Verfügung.

Mit freundlichen Grüssen
proFonds, Dachverband gemeinnütziger Stiftungen der Schweiz

Dr. Christoph Degen
Geschäftsführer

Sebastian Rieger
Recht und Steuern

RAIFFEISEN

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

Für Sie zuständig:
Dr. Hilmar Gernet – 079 750 77 29
hilmar.gernet@raiffeisen.ch

Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

14. Oktober 2021

Sehr geehrte Frau Bundesrätin
Sehr geehrter Herr Amstutz

Mit der Eröffnung der Vernehmlassung vom 23. Juni 2021 laden Sie interessierte Kreise ein, Stellung zu nehmen zum Entwurf für die Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG). Diese Gelegenheit nimmt Raiffeisen gerne wahr.

Zusammenfassend können wir Folgendes festhalten:

Raiffeisen ist der Ansicht, dass die vom Parlament in der verabschiedeten Version des revidierten Datenschutzgesetzes (revDSG) eingeschlagene Stossrichtung im E-VDSG deutlich zu wenig Berücksichtigung findet und teilweise im Widerspruch dazu steht. So haben Bestimmungen, welche vom Parlament aus der Gesetzesvorlage gestrichen wurden, im E-VDSG wieder Eingang gefunden. Der Verordnungsentwurf beinhaltet in der Folge nicht nur Ausführungsvorschriften zum Gesetz, sondern verschiedene Verschärfungen und Zusatzvorschriften im Vergleich zur europäischen Regulierung («Swiss Finish»), für welche das revDSG keine Grundlage vorsieht. Ausserdem bedürfen einige Bestimmungen einer Präzisierung. Der E-VDSG muss unter Berücksichtigung des revDSG und insbesondere der politisch intensiv geführten Diskussion, welche zu zahlreichen Kompromissen im Parlament geführt hat, überarbeitet werden. Im Einzelnen hat Raiffeisen nachfolgende Bemerkungen:

Art. 1 (Angemessenheit der Massnahmen):
In Abs. 1 Bst. d schlagen wir vor, «Implementierungskosten» durch «Implementierungsaufwand» zu ersetzen. Massgebend muss der Aufwand insgesamt sein (insbesondere auch in personeller Hinsicht). Die Beurteilung der Angemessenheit auf das Kriterium der Kosten zu beschränken, greift zu kurz.

Art. 1 (Prüfung der Massnahmen):
In Abs. 2 empfehlen wir, «in angemessenen Abständen» durch «in angemessener Weise» zu ersetzen. Eine Überprüfung sollte nicht zwingend nach einer bestimmten Zeitdauer vorgenommen werden müssen, sondern immer dann, wenn es angezeigt ist, beispielsweise bei einer Veränderung der Risikofaktoren.

Art. 2 (Schutzziele):
Wir empfehlen, Schutzziele «erreichen» durch «anstreben» zu ersetzen. Dies dürfte mit Blick auf die Formulierung im Einleitungssatz («angemessen») auch gemeint sein.

Art. 3 (Protokollierung):
Wie bereits eingangs ausgeführt, fehlen Grundlagen im revDSG, weshalb die Bestimmung zu streichen ist. Ausserdem erachten wir sie als verzichtbar, da das Bearbeitungsverzeichnis diese Funktion übernimmt.

Art. 4 (Bearbeitungsreglement):
Wir empfehlen die Streichung dieser Bestimmung, da im Gesetz keine Grundlage dafür existiert. Die Erstellung und Pflege eines solchen Reglements wäre mit einem unverhältnismässigen Aufwand verbunden. Ausserdem könnten betroffene Personen versuchen, vor- oder ausserprozessual über ein Auskunftsbegehren an das Bearbeitungsreglement zu gelangen. Dafür würden sie sich auf die Generalklausel des Auskunftsrechts stützen, die im Verbund mit der Strafbestimmung von Art. 62 revDSG (Verletzung der beruflichen Schweigepflicht) rechtsstaatlich hochproblematisch ist.

Ausserdem spricht die Historie gegen diese Bestimmung. Der aktuelle Art. 11 VDSG sollte damit offenbar in die neue VDSG übertragen werden, was jedoch unnötig ist und einen «Swiss Finish» darstellt, da die DSGVO keine solche Pflicht kennt. Sodann ist Abs. 3 missverständlich und täuscht darüber hinweg, dass Private nicht zwingend einen Datenschutzberater bestellen müssen.

Art. 6 (Auftragsbearbeiter):
Wir empfehlen, in Abs. 1 «sicherstellen» durch beispielsweise «Sorge tragen» oder «darauf hinwirken» zu ersetzen, da es dem Verantwortlichen nicht in jedem Einzelfall möglich sein wird, sicherzustellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.

Art. 8 (Angemessenheit Datenschutz Ausland):
Wir empfehlen eine Präzisierung, wonach sich die Abs. 1, 3 und 6 nur an den Bundesrat richten, da der Bundesrat festlegt, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten. Die Bestimmung kann ansonsten dahingehend missverstanden werden, dass die verantwortliche Stelle die Angemessenheit des Datenschutzes im Empfängerstaat prüfen muss.

Art. 10 (Standarddatenschutzklauseln):
Wir empfehlen, in Abs. 1 «sicherstellen» durch beispielsweise «Sorge tragen» oder «darauf hinwirken» zu ersetzen, da es dem Verantwortlichen nicht in jedem Einzelfall möglich sein wird, sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln beachtet.

Art. 13 (Modalitäten Pflichten):
Wir empfehlen, die Informationspflicht nur dem Verantwortlichen aufzuerlegen. Dies entspricht auch dem Wortlaut von Art. 19 Abs. 1 revDSG (Der Verantwortliche informiert die betroffene Person…). Hinsichtlich «leicht zugänglicher Form» erachtet Raiffeisen den Besuch einer Website als zumutbar, sodass die Informationspflicht mittels Verankerung in den AGB erfüllt werden kann.

Art. 15 (Information bei der Bekanntgabe von Personendaten):
Wir empfehlen die Streichung dieser Bestimmung. Diese Pflicht ist in ihrer Tragweite ein «Swiss Finish» und kann nicht allein auf Verordnungsstufe geregelt werden, da sie zu einschneidend ist.

Art. 16 (Information über die Berichtigung, Löschung oder Vernichtung):
Wir empfehlen die Streichung dieser Bestimmung, da dafür keine gesetzliche Grundlage vorliegt. Diese Pflicht war zwar im Vorentwurf zum revDSG enthalten, wurde dann aber im Rahmen der Vernehmlassung gestrichen und hat in der Beratung keinen Eingang ins Gesetz gefunden.

Art. 18 (Form und Aufbewahrung der Datenschutz-Folgenabschätzung (DSFA)):
Wir empfehlen, «schriftlich» durch beispielsweise die Formulierung «oder in einer anderen Form, welche den Nachweis durch Text ermöglicht» zu ergänzen (so wie dies auch in anderen Erlassen gehandhabt wird). Ausserdem regen wir an, zu konkretisieren, wann eine DSFA nötig ist und dafür Kriterien aufzuführen.

Art. 19 (Meldung von Verletzungen der Datensicherheit):
Wir empfehlen, in Abs. 1 die Bst. b.-d. zu streichen und eine Anpassung an die Europäische Datenschutz-Grundverordnung zu machen. Zu überlegen ist in Abs. 5 eine Reduktion der Frist auf zwei Jahre.

Art. 20 (Modalitäten):
Wir schlagen vor, die Dokumentationspflicht für die Gründe betr. Verweigerung der Aufbewahrung gemäss Abs. 5 zu streichen. Diese ist nicht nötig und hätte ansonsten im Gesetz verankert werden müssen. Ausserdem scheint die Aufbewahrungspflicht von drei Jahren zu lang bzw. eine Frist von zwei Jahren angemessener.

Art. 22 (Frist):
In Abs. 1 empfehlen wir folgende Präzisierung: Wenn aus dem Auskunftsbegehren nicht hervorgeht, welche Daten der Betroffene wünscht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.

Unabhängig von den obigen Ausführungen ist es angezeigt, dass für umfangreiche Anforderungen sachgerechte Übergangsfristen definiert werden, beispielsweise für Vertragsanpassungen, die Durchführung von Datenschutz-Folgenabschätzungen und ggf. Dokumentationspflichten.

Für weitere Anliegen verweisen wir auf die ausführliche Stellungnahme von economiesuisse, welche wir inhaltlich mittragen.

Für die Gelegenheit zur Stellungnahme bedanken wir uns bestens. Wir bitten um Berücksichtigung der Anliegen von Raiffeisen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Dr. Hilmar Gernet
Delegierter für Public Affairs und Geschichte

Christian Bopp
Leiter Regulatory & Reporting

Schweizerische Rettungsflugwacht
Garde aérienne suisse de sauvetage
Guardia aerea svizzera di soccorso

Postfach 1414, CH-8058 Zürich-Flughafen

Betrieb

Schweizerische Rettungsflugwacht Rega
Rega-Center
Postfach 1414
CH-8058 Zürich-Flughafen

Tel. +41 44 654 33 11
Fax +41 44 654 33 22
www.rega.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik
Bundesrain 20
3003 Bern

Von Markus Ritter
E-Mail markus.ritter@rega.ch
Datum 29. September 2021
Betreff Stellungnahme zur Totalrevision VDSG

Sehr geehrte Damen und Herren

Nachfolgend nimmt die Schweizerische Rettungsflugwacht Rega Stellung zum Entwurf der Verordnung zum Datenschutzgesetz.

Die Rega bearbeitet bei der Erfüllung ihrer Aufgaben regelmässig Personendaten, die zu einem wesentlichen Teil als Gesundheitsdaten besonders schützenswert sind. Aus diesem Grund ist es für die Rega wichtig, dass die datenschutzrechtlichen Grundlagen, die dabei anzuwenden sind, klare Vorgaben enthalten und in der Praxis nicht zu unnötigen Komplikationen führen.

Wir haben daher den Entwurf der Verordnung zum Datenschutzgesetz des Bundes (E-VDSG) eingehend studiert und erlauben uns im Folgenden einige Hinweise.

Wir haben festgestellt, dass der E-VDSG zusätzliche Dokumentationspflichten enthält, die die unternehmensinternen Abläufe komplizieren, ohne gleichzeitig einen entsprechenden Mehrwert für den Schutz der Persönlichkeitsrechte der betroffenen Personen zu bieten.

Zudem enthält die Verordnung einige Bestimmungen, welchen die gesetzliche Grundlage fehlt, oder die sogar dem Willen des Gesetzgebers widersprechen (z.B. bei den neu eingeführten Dokumentationspflichten).

Nachfolgend gehen wir auf einzelne Bestimmungen ein.

1. Datensicherheit / Dokumentationspflichten

Betreffend die Datensicherheit führt **Art. 2 E-VDSG** die Schutzziele auf. Diese Liste ist jedoch veraltet und zu detailliert formuliert. Die Regelung zwingt zu einer Dokumentation für jede Datenbearbeitung. Das widerspricht dem Willen des Gesetzgebers, der eine solche umfassende Dokumentationspflicht abgelehnt hat.

Da die Einhaltung der Mindestanforderungen an die Datensicherheit nach dem revDSG mit Strafe bedroht ist, erscheint uns eine klare Regelung dieses Punktes als ausserordentlich wichtig. Die Rega ist der Meinung, dass dieses Ziel mit der vorgeschlagenen Regelung nicht erreicht wurde.

Die in **Art. 3 Abs. 1 E-VDSG** vorgesehene Protokollierungspflicht und die in **Art. 3 Abs. 4 E-VDSG** vorgesehene Regelung der getrennten Aufbewahrung sind zudem technisch nicht ohne Weiteres oder nur mit erheblichem Aufwand umsetzbar. Protokolle werden dort erzeugt, wo sie anfallen – und nicht auf anderen Systemen. Die Rega müsste somit von sämtlichen Protokollen Kopien anfertigen und sie manuell auf ein anderes System übertragen. Dadurch entstehen Sicherheitsrisiken und es ist mit einem enormen Aufwand verbunden. Es würde genügen, wenn sichergestellt wird, dass die Protokolle ihrerseits sicher sind. Dieser Bestimmung fehlt ausserdem die gesetzliche Grundlage. Auch für die Aufbewahrungspflicht von 2 Jahren gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet.

Die in **Art. 4 E-VDSG** vorgesehene Pflicht zur Erstellung eines Bearbeitungsreglements für Datenbearbeitungen mit einem hohen Risiko ist nach Ansicht der Rega abzulehnen, da sie zu einem unnötigen Dokumentationsaufwand und zu einem erheblichen administrativen Aufwand führen wird. Die wesentlichen Angaben einer geplanten Datenbearbeitung sind bereits im Rahmen der Datenschutz-Folgenabschätzung zu dokumentieren, daher ist die Regelung unseres Erachtens überflüssig. Zudem fehlt dieser Regelung gemäss unserer Einschätzung die gesetzliche Grundlage.

2. Informationspflichten

Für die «Informationspflicht bei der Bekanntgabe von Personendaten» gemäss **Art. 15 E-VDSG** fehlt ebenfalls die gesetzliche Grundlage. Gegenüber der bisherigen Regelung in der VDSG wird die Vollständigkeit neu hinzugefügt, d.h. die Daten dürfen nicht lückenhaft sein. Die Regelung ist praxisfremd und lässt sich nicht vernünftig umsetzen. Hinzu kommt, dass der Empfänger ohnehin selbst verpflichtet ist, die Bearbeitungsgrundsätze einzuhalten und angemessene Massnahmen zu treffen, sich über die Richtigkeit der Daten zu vergewissern.

Die in **Art. 16 E-VDSG** vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von

Personendaten zu informieren, war bereits im Entwurf des revDSG vorgesehen und wurde vom Parlament gestrichen. Die Einführung dieser Pflicht über die revidierte Verordnung würde daher dem Willen des Parlaments widersprechen. Dieselbe Bestimmung verweist zudem auf ein Recht auf Einschränkung der Bearbeitung von Personendaten, das so im revDSG nicht besteht.

Art. 19 Abs. 5 E-VDSG möchte eine Dokumentationspflicht einführen, die zwar in der DSGVO, nicht aber im revDSG vorgesehen wird. Daher kann sie und die entsprechende Aufbewahrungspflicht auch nicht auf dem Weg der Verordnung eingeführt werden.

3. Fazit

Wir sind daher der Ansicht, dass der gegenwärtige Entwurf einer grundsätzlichen Überarbeitung bedarf. Es sollten ausserdem noch Übergangsfristen von 1 Jahr ab Inkrafttreten des revDSG für die Erstellung der Verzeichnisse und – falls darauf entgegen den Anträgen nicht verzichtet wird – auch für das Bearbeitungsreglement vorgesehen werden.

Wir bedanken uns im Voraus für die Berücksichtigung unserer Rückmeldung. Zur Beantwortung von Fragen zu dieser Stellungnahme steht Ihnen Markus Ritter, Informationssicherheitsbeauftragter, gerne zur Verfügung.

Freundliche Grüsse
Schweizerische Rettungsflugwacht Rega

Ernst Kohler
CEO / Vorsitzender der Geschäftsleitung

Andreas Lüthi
CFO / Mitglied der Geschäftsleitung

Ringier We inform. We entertain. We connect.

per E-Mail an:
fanny.matthey@bj.admin.ch
daniela.nueesch@bj.admin.ch

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, 14. Oktober 2021

Stellungnahme zum Vorentwurf der Verordnung zum Bundesgesetz über den Datenschutz (VE-VDSG)

Sehr geehrte Frau Matthey,
Sehr geehrte Frau Nüesch,
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf das Vernehmlassungsverfahren zum Vorentwurf der Verordnung zum Bundesgesetz über den Datenschutz (nachfolgend “VE-VDSG”) und nehmen hiermit gerne die Gelegenheit wahr, termingerecht Stellung zum genannten Vorentwurf zu nehmen.

Die Ringier AG ist ein aktives Mitglied des Vereins Unternehmens-Datenschutz (nachfolgend “VUD”), der eine detaillierte Stellungnahme zum VE-VDSG eingereicht hat. Die Ringier AG schliesst sich deshalb der Stellungnahme des VUD an und beschränkt sich in der Folge nur auf einige wesentliche Anmerkungen zum VE-VDSG.

T +41 44 259 61 11
F +41 44 259 68 40

www.ringier.com

Ringier AG
Dufourstrasse 23
CH-8008 Zürich
Schweiz

T +41 44 259 61 11
F +41 44 259 68 40

www.ringier.com

Grundsätzlich wurde bei der Sichtung des VE-VDSG festgestellt, dass im Rahmen der Ausformulierung des VE-VDSG teilweise neue Pflichten geschaffen wurden (z.B. Dokumentationspflichten, Bearbeitungsreglement, Protokollierungspflicht, usw.), welche keine Delegationsnorm im revidierten Bundesgesetz über den Datenschutz (nachfolgend “revDSG”) zur Grundlage haben. Diese Vorgaben müssen gestrichen werden, da sich der VE-VDSG als Verordnung naturgemäss auf die Ausführungsvorgaben aus dem revDSG beschränken soll.

Des Weiteren ist davon abzusehen, Vorgaben im Rahmen der Revision der VDSG einzuführen, welche im Revisionsprozess des Bundesgesetzes über den Datenschutz bewusst gestrichen wurden, so zum Beispiel eine allgemeine Dokumentationspflicht (Art. 19 Abs. 5 VE-VDSG).

In mehreren Vorgaben des VE-VDSG wurde zudem auf dieselben Formulierungen oder Konzepte aus der heute geltenden VDSG und deren Botschaft zurückgegriffen, welche heute unter der Berücksichtigung der technologischen Weiterentwicklung als nicht mehr sinnvoll erscheinen. Insbesondere in Bezug auf die Datensicherheit wurden die sehr detaillierten, heute geltenden Vorgaben bezüglich der technischen und organisatorischen Massnahmen übernommen, ohne jedoch das grundlegende Konzept der heute gelebten Datensicherheit und deren Schutzziele: Integrität, Vertraulichkeit und Verfügbarkeit, zu verankern. Im Hinblick darauf, dass die Revision der heute geltenden Datenschutzgesetzgebung in Schweiz eine Modernisierung und vor allem eine Anpassung an die heutigen sowie zukünftigen technologischen Entwicklungen zum Ziel hat, empfehlen wir die revisionsbedürftigen Konzepte sowie der erwähnte Katalog der Schutzziele betreffend Datensicherheit aus der geltenden VDSG zu überarbeiten. Letzterer anzupassen scheint uns besonders wichtig, da die Verletzung der Mindestanforderungen an die Datensicherheit zukünftig mit Strafe bedroht ist (Art. 61 lit. c. revDSG).

Abschliessend möchten wir darauf hinweisen, dass durch den VE-VDSG keine Vorgaben geschaffen werden sollten, welche über die hohen Anforderungen der Europäischen Datenschutz-Grundverordnung (nachfolgend “DSGVO”) hinausgehen. Im Hinblick darauf, dass es im VE-VDSG mehrere “Swiss-Finish” gibt, so z.B. Art. 15 VE-VDSG (Information bei der Bekanntgabe von Personendaten) beantragen wir deren Streichung. Es war - aus nachvollziehbaren Gründen - die Absicht des Schweizer Gesetzgebers, das heute geltende DSG auf ein höheres Niveau anzuheben und an die Anforderungen der DSGVO anzupassen. Es war und kann aber nicht das Ziel sein, höhere Hürden für Schweizer Unternehmen zu schaffen und sie damit im Hinblick auf die Unternehmen im EWR zu benachteiligen - dies insbesondere nicht im Rahmen einer Revision einer Verordnung.

Wir danken Ihnen für die Gelegenheit der Stellungnahme und die Berücksichtigung unserer ausgeführten Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Ringier AG

Chantal Imfeld-Matyàssy

Chantal Imfeld-Matyassy
Head of Data Protection & Data Protection Officer Ringier Gruppe

Manuel Liatowitsch
Group General Counsel / Chief Legal Officer & Head of Corporate Center

Per Email:
jonas.amstutz@bj.admin.ch

Bern, 11. Oktober 2021 Si

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) Stellung nehmen zu dürfen.

Der Reifen-Verband der Schweiz (RVS) vertritt auf nationaler Ebene die Interessen des Reifenfachhandels, der Reifenimporteure sowie der Altreifen-Entsorgungsbetriebe. Unsere Mitglieder sind vorwiegend Klein- und Mittelbetriebe. Wir plädieren daher grundsätzlich für KMU-verträgliche und in der Praxis mit verhältnismässigem Aufwand umsetzbare Lösungen, welche auf die personellen und finanziellen Ressourcen der Betriebe Rücksicht nehmen.

A. Das VDSG als Instrument zur Erreichung der Euro-Kompatibilität

Wie beim DSG hat der Bundesrat auch beim E-VDSG in seinen Erläuterungen festgehalten, dass es lediglich um die Angemessenheit des Schweizerischen Datenschutzrechts im Vergleich zur europäischen DSGVO geht. In keiner Art und Weise wurde je von einer Erweiterung der Einschränkungen bei den Datenbearbeitungen bzw. von einer strengeren Regelung gesprochen. Diesem Ziel bleibt der Bundesrat auch bei der Formulierung der VDSG ausdrücklich verpflichtet. Alle Bestimmungen, welche folglich über die Erfordernisse der DSGVO hinausgehen müssen als zweckfremd und als unzulässig abgelehnt werden. Diese sind konsequent aus dem E-VDSG zu löschen.

B. Formelle Bemerkung

Zur besseren Lesbarkeit der Verordnung und zum klareren Bezug zum DSG würden wir klare Verweise auf die betroffenen Gesetzesbestimmungen im Titel der jeweiligen Bestimmungen begrüssen.

C. Zu den einzelnen Bestimmungen

Art. 1 Abs. 1 Bst. d

In Art. 1 Bst. d werden als Kriterium der Angemessenheit für die Datensicherheit die «Implementierungskosten» genannt. Es wird begrüsst, dass der Aufwand für die Verantwortlichen auch ausdrücklich in die Angemessenheitsüberprüfung aufgenommen wird. Der verwendete Begriff erscheint jedoch problematisch, da er lediglich auf die geldwerten Umsetzungsaufwendungen beschränkt werden könnte (siehe auch S. 16 der Erläuterungen). Für eine solche Einschränkung gibt es keinen Grund. Statt den Begriff «Implementierungskosten» schlagen wir vor, den allgemeineren Begriff «Aufwand für den Verantwortlichen» zu verwenden. Es gibt keinen Grund, beim Verantwortlichen überhöhte Planungs- oder Projektkosten auszulösen, nur um festzustellen, ob die Implementierung dann ihrerseits verhältnismässig ist.

Art. 1 Abs. 2

Diese Bestimmung verlangt die Überprüfung der technischen und organisatorischen Massnahmen in angemessenen Abständen (gemeint sind hier die zeitlichen Abstände). Aufgrund des risikobasierten Ansatzes der gesamten Thematik der Datensicherheit erscheint diese Regelung falsch. Zudem ist fraglich, ob mit der vom Bundesrat aufgestellten Forderung der Überprüfung in angemessenen Abständen die Delegationsnorm von Art. 8 Abs. 3 DSG eingehalten wird. Die Mindestanforderungen an die Datensicherheit rechtfertigen keine Einführung von zusätzlichen Kriterien, welche im Gesetz nicht verankert sind. Es ist - wenn überhaupt - in materieller Hinsicht zu fordern, dass ein Zusammenhang zwischen der Überprüfung der Datensicherheit und der Entwicklung des Risikos hergestellt wird.

➔ Formulierungsvorschlag: «Die Massnahmen sind bei einer relevanten Veränderung des Risikos zu überprüfen.»

Art. 2 Einleitungssatz

Die Bestimmung spricht von «Schutzzielen erreichen». Die Pannen der Swisscom zeigen mit aller Deutlichkeit auf: Die absolute Datensicherheit gibt es nicht. Von den Verantwortlichen zu verlangen, dass die entsprechenden Schutzziele erreicht werden, ist weder korrekt noch realistisch. Der Bereich der Datensicherheit ist ein typischer Bereich, bei welchem keine Ergebnisverantwortung, sondern nur eine Sorgfaltspflicht auferlegt werden darf.

➔ Formulierungsvorschlag: «Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele anstreben: (…)»

Nur so dürfen in der nachfolgenden Aufzählung Begriffe wie «verwehrt», «verunmöglicht», «verhindert», «gewährleistet», usw. überhaupt verwendet werden. Ansonsten müssten in der Aufzählung die Schutzziele jeweils vernünftig relativiert werden.

Art. 2 Bst. a bis k

Art. 2 dürfte eigentlich nur Schutzziele nennen, welche vom Verantwortlichen beeinflusst werden können. Gerade die Transportkontrolle kann beispielsweise durch viele externe Faktoren gefährdet werden, für welche der Verantwortliche nicht einstehen kann. Die Aufzählung von Art. 2 Bst. a bis k zeigt, was in der Lehre verschiedentlich moniert worden ist: Mangels Effizienz der staatlichen Interventionen, wird die Last der «Privacy by design» vollumfänglich auf den Verantwortlichen abgewälzt, statt dass sie zu datenschutzfreundlichen Technologien durch die Hersteller von Hard- und Software führen würde. Diese Entwicklung zulasten der Nutzer von Informationstechnologien ist problematisch, da damit auch der Aufwand für die Datensicherheit

dem Betreiber und nicht dem Entwickler von Informationstechnologien auferlegt wird. Die Aufzählung in Art. 2 Bst. a bis k ist in Beachtung dieser Problematik zu überarbeiten und dem Verantwortlichen dürfen nur Schutzziele auferlegt werden, die auch tatsächlich in seiner Verantwortung liegen.

Art. 3
Die nun in der Verordnung vorgesehenen Anforderungen an die Protokollierung übersteigen das vernünftige Mass und führen zu einer Bürokratie, welche in keinem Verhältnis zum tatsächlichen Nutzen der Anforderungen steht. Insbesondere die Aufbewahrungsdauer der Protokolle von 2 Jahren (Art. 3 Abs. 4 E-VDSG) ist unangemessen.
Aus Sicht der Wirtschaft genügt die Pflicht zur Erstellung eines Verzeichnisses der Datenbearbeitungen vollumfänglich, um die Rechte und die Interessen der betroffenen Personen zu wahren.

Art. 4
Die Anforderungen von Art. 4 E-VDSG gehen zu weit. Ein Bearbeitungsreglement wird abgelehnt. Sollte wider Erwarten am Bearbeitungsreglement festgehalten werden, gibt es keinen nachvollziehbaren Grund zur «regelmässigen» Überarbeitung desselben. Dieses muss dann überarbeitet werden, wenn es einen Anlass zur Aktualisierung gibt (Veränderung der Bearbeitungsmittel oder Formen).

Art. 6 Abs. 1 und 2
Die Pflicht, für den Verantwortlichen, die vertrags- und gesetzesmässige Bearbeitung durch den Auftragsbearbeiter «sicherzustellen» ist konzeptionell falsch. Richtig ist, dass der Verantwortliche sich gemäss Art. 9 Abs. 2 DSG vergewissern muss, dass die Datenbearbeitung korrekt erfolgt. Diese unverhältnismässige, nicht einzuhaltende und nicht vom Gesetzgeber vorgesehene Verschärfung der Pflicht des Verantwortlichen ist im Rahmen der Delegation an den Bundesrat als zu weit gehend zu betrachten.

➔ Formulierungsvorschläge für Art. 6 Abs. 1 2. Satz bzw.
Art. 6 Abs. 2 2. Satz E-VDSG:
Er vergewissert sich, dass die Daten vertrags- und gesetzesgemäss bearbeitet werden.
Andernfalls muss er sich auf dem vertraglichen Weg vergewissern, dass ein gleichwertiger Datenschutz gewährleistet wird.

Art. 9 Abs. 2 und Art. 10 Abs. 1
Auch diese Forderung an den Verantwortlichen geht zu weit, wenn er «sicherstellen» muss. Der Terminus «vergewissern» ist zu verwenden.

Art. 15 und 16
Diese Bestimmungen finden keine Grundlage im DSG und sind ersatzlos zu streichen. Die Berichtigung, Löschung, Vernichtung oder Einschränkung der Bearbeitung von Personendaten (Art. 16 E-VDSG) erfolgen zudem im Interesse der betroffenen Person. Diese müssen ja so oder so den Anforderungen des Gesetzes entsprechen. Wieso in solchen Situationen eine neue Informationspflicht im Interesse der betroffenen Person liegen soll, ist nicht klar. Im Gegenteil: Mit einer solchen Information, sei sie auch noch so klar, wird die betroffene Person oft verunsichert oder zumindest auf einen Umstand aufmerksam gemacht, der dazu führt, dass Fragen aufgeworfen werden und Aufwand generiert wird, der dem Verantwortlichen nicht entschädigt wird.

Das wird von der Wirtschaft in nachvollziehbarer Weise als unnötige und bürokratische Zusatzbelastung empfunden. Auf unnötige Informationen ist in den Beziehungen zwischen dem Datenbearbeiter und der betroffenen Person zu verzichten.

Art. 18
Die Aufbewahrungsfrist von 2 Jahren nach Beendigung der Datenbearbeitung entbehrt einer gesetzlichen Grundlage im DSG und ist als zu lange zu betrachten. Die Aufbewahrung hat höchstens bis zur Beendigung der entsprechenden Datenbearbeitung zu dauern, da danach keine Verletzung der Rechte der betroffenen Person mehr erfolgen kann. Für die Frage, ob jemand durch die Datenbearbeitung ein Schutzrecht der betroffenen Person verletzt hat, ist nicht die Datenschutz-Folgenabschätzung relevant, sondern die konkrete Datenbearbeitung und die entsprechenden Verzeichnisse und Reglemente des Verantwortlichen.

Art. 19 Abs. 1 Bst. b bis d
Diese Kriterien sind dem Gesetz nicht zu entnehmen. Der Bundesrat hat weder eine Delegation noch eine Ermächtigung erhalten, Art. 24 DSG zu ergänzen. Deshalb sind diese Buchstaben aus der Verordnung zu streichen.

Ar. 19 Abs. 1 Bst. e
Bei der Entdeckung einer Verletzung der Datensicherheit ist es eben gerade nicht immer möglich, die Folgen und die allfälligen Risiken umgehend und abschliessend festzustellen. Deshalb muss beim Bst. e «*soweit möglich*» vorangestellt werden.

Art. 19 Abs. 3
Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 Abs. 4 DSG hinausgeht.

Art. 19 Abs. 5
Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wider Erwarten an einer Dokumentationspflicht festhalten, sind die 3 Jahre deutlich zu lang. Eine Aufbewahrungsdauer soll höchstens ein Jahr betragen.

Art. 20 Abs. 5
Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 25 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wider Erwarten an einer Dokumentationspflicht festhalten, sind die 3 Jahre zu lang. Eine Aufbewahrungsdauer soll höchstens ein Jahr betragen.

Art. 22
Der Fristenlauf kann erst dann beginnen, wenn das Auskunftsgesuch formell korrekt eingereicht und inhaltlich klar ist. Solange das Gesuch entweder formell oder inhaltlich unklar ist, kann die Frist nicht laufen. Dies muss im Art. 22 E-VDSG in aller Klarheit zum Ausdruck kommen.

Art. 23
Aufgrund der Einschränkungen, die gemäss Abs. 1 für die Kostenbeteiligung vom Bundesrat aufgestellt werden, steht der Betrag von CHF 300 in keiner vernünftigen Relation zum «unverhältnismässigen Aufwand». Bei Aufwendungen, die weit über CHF 1'000 gehen können, ist eine Kostenbeteiligung von nur gerade CHF 300 nicht angemessen. Natürlich hat der Verantwortliche die Kosten zu belegen. Aber es kann nicht sein, dass der Verantwortliche auf seinen Kosten sitzenbleibt und vom Kostenverursacher nur quasi ein symbolischer Betrag verlangt werden kann. Der Höchstbetrag ist deshalb anzuheben und sollte auf mindestens CHF 1'000 festgelegt werden.

Art. 24
Der Anspruch auf Datenportabilität bei der Datenherausgabe oder -übertragung, darf nicht ein absoluter sein. Dieser Anspruch darf nur bestehen, soweit die Bearbeitung von Personendaten in gängigen Formaten erfolgen kann bzw. erfolgt.

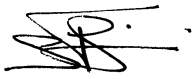
Art. 45 Abs. 1 und 2
Wenn die Kostenbeteiligung nach Art. 23 mit den Gebührengrundsätzen des EDÖB verglichen werden, dann muss von einer krassen Diskrepanz gesprochen werden. Der EDÖB erledigt eine Tätigkeit im Interesse der Gesellschaft und es gibt keinen nachvollziehbaren Grund, weshalb die Person, welche Dienstleistungen von ihm in Anspruch nehmen muss, um sich datenschutzkonform zu verhalten, derart hohe Gebühren zu bezahlen hat. Weder kann es sein, dass die Gebühren nach Zeitaufwand berechnet werden (die Privatperson hat keinen Einfluss auf die Effizienz der Leistungserbringung durch den EDÖB), noch sind die Stundensätze von CHF 150 bis 350 angemessen. Diese Gebührenbestimmung stiftet die hilfesuchende Privatperson geradezu an, das Datenschutzrecht zu verletzen, da sie sich die Unterstützung durch den EDÖB nicht leisten kann. Die Gebührenordnung ist vollständig zu überdenken und auf ein vernünftiges Mass anzupassen. Hier wird dem Service-Public-Gedanken zu wenig Rechnung getragen. Es ist erforderlich, Maximalgebühren für Tätigkeiten festzulegen, welche der Einhaltung des Datenschutzrechts dienen (z.B. Art. 59 Abs. 1 Bst. c DSG, Konsultation aufgrund einer Datenschutz-Folgenabschätzung).

Wir bitten Sie um Kenntnisnahme und danken für eine Berücksichtigung unserer Anliegen bestens.

Freundliche Grüsse

REIFEN-VERBAND DER
SCHWEIZ RVS

Der Präsident



Sven Sievi

santésuisse
Römerstrasse 20
Postfach 1561
CH-4502 Solothurn
Tel. +41 32 625 41 41
Fax +41 32 625 41 51
mail@santesuisse.ch
www.santesuisse.ch

santésuisse | Die Schweizer Krankenversicherer
Les assureurs-maladie suisses

Für Rückfragen:
Agnes Stäuble
Direktwahl: +41 32 625 4266
Agnes.Staeuble@santesuisse.ch

Solothurn, 14. Oktober 2021

Vernehmlassungsverfahren zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Stellungnahme santésuisse

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellung nehmen zu können.

santésuisse befürwortet eine für die Anwender klare und durchdachte Revision sowohl des Datenschutzgesetzes als auch der dazugehörigen Verordnung. Die nun vorliegende Verordnungsvorlage beinhaltet jedoch zum Teil ungenaue Begrifflichkeiten sowie Doppelspurigkeiten. Damit eine einheitliche Handhabung in der Umsetzung gewährleistet werden kann, sind diese zu präzisieren bzw. zu korrigieren. Gerne geben wir unsere entsprechenden Anregungen in der nachfolgenden Tabelle.

Weiter stellt die VDSG eine unselbstständige Verordnung dar. Das heisst, sie bedarf einer Grundlage im Gesetz. santésuisse stellt fest, dass dieser Umstand in der vorliegenden Vernehmlassungsvorlage mehrfach unberücksichtigt geblieben ist. Beispielsweise sieht das Datenschutzgesetz

in Art. 12 neu das Führen eines Bearbeitungsverzeichnisses vor. Dieses ersetzt inhaltlich das bisherige „Bearbeitungsreglement“, welches die Krankenversicherer weiterhin gemäss Art. 84b KVG erstellen und veröffentlichen müssen. Ohne entsprechende gesetzliche Grundlage wird nun neu in Art. 4 VDSG zusätzlich zum Bearbeitungsverzeichnis gemäss Art. 12 revDSG die Erstellung eines Bearbeitungsreglements verlangt. Die Krankenversicherer werden also zu einem Doppelaufwand verpflichtet, ohne jeglichen Nutzen. Vor diesem Hintergrund drängt sich zusätzlich auch noch die Frage auf, ob in der Gesetzesrevision allenfalls vergessen wurde, die Korrelation zu Art. 84b KVG zu klären.

Bitte entnehmen Sie der nachfolgenden Tabelle unsere Überlegungen und Vorschläge zu den einzelnen Bestimmungen:

Vorentwurf Teilrevision	**Vorschlag santésuisse**	**Bemerkungen**
Der Schweizerische Bundesrat, *gestützt auf die Artikel 8 Absatz 3, 10 Absatz 4, 12 Absatz 5, 16 Absatz 3, 25 Absatz 6, 28 Absatz 3, 33, 59 Absätze 2 und 3 des Bundesgesetzes vom 25. September 20201 über den Datenschutz (DSG)* *verordnet:*		
1. Kapitel: Allgemeine Bestimmungen		
1. Abschnitt: Datensicherheit		
Art. 1 Grundsätze [1] Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a. Zweck, Art, Umfang und Umstände der Datenbearbeitung; b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen; c. der Stand der Technik; d. Implementierungskosten.	d. Implementierungs**aufwand**.	**Zu lit. d:** Die Abwägung kann sich nicht nur auf die Implementierungskosten beschränken. Das macht keinen Sinn. Es ist der gesamte Implementierungsaufwand

		in die Abwägung einzubeziehen (auch personelle, zeitliche oder organisatorische Aufwendungen).
[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.	[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg **gemessen an den zugrunde liegenden Risiken regelmässig** zu überprüfen.	**Zu Abs. 2:** Die Überprüfung hat nicht nur in angemessenen Abständen, sondern insbesondere in angemessener Weise zu erfolgen. Wenn sich die Risikofaktoren nicht ändern, bedarf es keiner entsprechenden Überprüfung.
Art. 2 Schutzziele Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen: a. Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen. b. Zugangskontrolle: Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt.	Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele **anstreben**:	**Zu Art. 2:** Die Verwendung des Worts «erreichen» impliziert, dass die Schutzziele vollständig erfüllt werden, was weder erforderlich noch möglich ist. Zu treffen sind nur angemessene Massnahmen.
c. Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht. d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert. e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungs-systemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert. f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.	c. Datenträgerkontrolle: Das **Bearbeiten** von Datenträgern wird unbefugten Personen verunmöglicht. d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugtes **Bearbeiten** gespeicherter Personendaten wird verhindert. f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt **bearbeitet** werden können.	**Zu lit. c, d und f:** Die hier aufgeführten Begriffe definiert das revDSG in Art. 5 lit. d als „Bearbeiten“. Der Vollständigkeit sowie der Einfachheit halber ist diese Begriffsdefinition zu übernehmen. Weiter ist nicht klar, was der Unterschied zwischen den beiden Begriffen „Datenträger“ und „Datenspeicher“ ist. Unserer Meinung nach haben die beiden Begriffe dieselbe Bedeutung.

g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden. h. Bekanntgabekontrolle: Es kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden. i. Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden. j. Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität). k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.		
Art. 3 Protokollierung [1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. [2] Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das	~~**Art. 3 Protokollierung**~~ ~~[1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.~~ ~~[2] Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das~~	**Zu Art. 3:** Diese Bestimmung ist in mehrerlei Hinsicht problematisch und sollte ersatzlos gestrichen werden: Erstens fehlt ihr eine gesetzliche Grundlage. Zweitens ist das Ergebnis der Datenschutz-Folgenabschätzung (DSFA) kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. In der Regel wird eine DSFA aufgrund der Art und Weise der Datenbearbeitung vorgenommen. Drittens muss eine solche Bearbeitung kraft Art. 21 revDSG ohnehin dem EDÖB oder Datenschutzberater vorgelegt werden. Eben dies dient bereits dem

Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. 3 Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist. 4 Die Protokolle sind während zwei Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.	~~Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.~~ ~~3 Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.~~ ~~4 Die Protokolle sind während zwei Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.~~	Ziel, eine solche oder andere Massnahme vorzuschlagen, soweit die Bearbeitung überhaupt umgesetzt werden kann. Viertens obliegt die Pflicht auch dem Auftragsbearbeiter, der jedoch die DSFA nicht kennen muss und eine solche schon gar nicht auszuführen hat. Massnahmen zur Datensicherheit obliegen zwar auch ihm, aber diese Protokollierung ist in ihrem Kern keine solche. Das erklärt den unlösbaren Widerspruch. Auch deshalb ist sie zu streichen. Sollte der Artikel entgegen unserem Dafürhalten nicht gestrichen werden, stellen sich uns betreffend die einzelnen Absätze weitere Fragen: **Zu Abs. 1:** Insbesondere geht eine Protokollierung allein für das Lesen zu weit. Was bedeutet zudem „automatisierte Bearbeitung“? Das Gesetz verwendet diesen Begriff im Zusammenhang mit „Profiling“. Falls Profiling gemeint ist, könnte man diesen im Gesetz (Art. 5 lit. f revDSG) normierten Begriff übernehmen, damit der Begriff klar definiert ist. **Zu Abs. 3:** Es ist nicht klar, in welchem Verhältnis Abs. 3 zu Abs. 1 und 2 steht. Abs. 3 geht weiter. Zudem bestehen Unklarheiten in der Abgrenzung (Identität der Person, Identität des Empfängers). In der Praxis sind von dieser Bestimmung vor allem die IT-Mitarbeitenden erfasst. Wir gehen davon aus, dass diese hier miteingeschlossen sind, ansonsten bestünde ein Problem in der Umsetzung. Respektive ist der Personenkreis mit Zugang um

		jene im Wortlaut zu erweitern, welche die Verletzung von Datenschutzvorschriften verfolgen. Weiter stellen wir uns die Frage, weshalb die Protokolle während zwei Jahren aufbewahrt werden müssen? Der Datenschutz schreibt ja eigentlich vor, dass die Daten jeweils zu löschen sind, wenn sie nicht mehr benötigt werden. Aus unserer Sicht reicht deshalb die Aufbewahrung während eines Jahres. Respektive eine starre Frist macht keinen Sinn und wäre unverhältnismässig. Sie muss von der Dauer der Datenbearbeitung abhängig und generell angemessen sein.
Art. 4 Bearbeitungsreglement von privaten Personen [1] Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie: a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen. [2] Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. zur internen Organisation; e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe;	~~**Art. 4 Bearbeitungsreglement von privaten Personen**~~ ~~[1] Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie:~~ ~~a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder~~ ~~b. ein Profiling mit hohem Risiko durchführen.~~ ~~[2] Das Reglement muss mindestens Angaben enthalten:~~ ~~a. zum Bearbeitungszweck;~~ ~~b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;~~ ~~c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;~~ ~~d. zur internen Organisation;~~ ~~e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung;~~ ~~f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit;~~ ~~g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe;~~	**Zu Art. 4** Das Gesetz sieht neu in Art. 12 das Führen eines Bearbeitungsverzeichnisses vor. Dieses ersetzt inhaltlich das bisherige „Bearbeitungsreglement“, welches die Krankenversicherer weiterhin gemäss Art. 84b KVG erstellen und veröffentlichen müssen. Indem nun neu in Art. 4 VDSG zusätzlich zum Bearbeitungsverzeichnis gemäss Art. 12 revDSG die Erstellung eines Bearbeitungsreglements verlangt wird, werden die Krankenversicherer zu einem Doppelaufwand verpflichtet, ohne jeglichen Nutzen. Wurde in der Gesetzesrevision allenfalls vergessen, die Korrelation zu Art. 84b KVG zu klären? Zudem fehlt für das Führen eines Bearbeitungsreglements eine gesetzliche Grundlage, da Art. 8 revDSG nur Datensicherheit i.e.S. regelt. Aus diesen Gründen lehnen wir Art. 4 ab.

h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung. 3 Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.	~~h. zu den Massnahmen, die zur Datenminimierung getroffen werden;~~ ~~i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung;~~ ~~j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.~~ ~~3 Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.~~	**Zu Abs. 3:** Abs. 3 geht zudem fälschlicherweise davon aus, dass immer ein Datenschutzberater zu bestellen ist. Diese Vorgabe ist für Privatpersonen aber optional! Das Bearbeitungsreglement des Privaten muss weder publiziert noch dem EDÖB gemeldet werden.
Art. 5 Bearbeitungsreglement von Bundesorganen 1 Das verantwortliche Bundesorgan und dessen Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie: a. besonders schützenswerte Personendaten bearbeiten; b. ein Profiling durchführen; c. Datenbearbeitungen im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG ausführen; d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen werden Personendaten zugänglich machen; e. Datenbestände miteinander verknüpfen; oder f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften. 2 Das Reglement muss mindestens die Angaben nach Artikel 4 Absatz 2 enthalten.	~~**Art. 5 Bearbeitungsreglement von Bundesorganen**~~ ~~1 Das verantwortliche Bundesorgan und dessen Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie:~~ ~~a. besonders schützenswerte Personendaten bearbeiten;~~ ~~b. ein Profiling durchführen;~~ ~~c. Datenbearbeitungen im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG ausführen;~~ ~~d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen werden Personendaten zugänglich machen;~~ ~~e. Datenbestände miteinander verknüpfen; oder~~ ~~f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.~~ ~~2 Das Reglement muss mindestens die Angaben nach Artikel 4 Absatz 2 enthalten.~~	**Zu Art. 5:** Vgl. unsere Bemerkungen zu Art. 4.

[3] Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen.	~~[3] Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen.~~	
2. Abschnitt: Bearbeitung durch Auftragsbearbeiter		
Art. 6 Modalitäten [1] Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden. [2] Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen. [3] Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich genehmigt hat.	[1] Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss **dafür sorgen**, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.	**Zu Abs. 1:** Der Verantwortliche kann nicht sicherstellen, dass der Auftragsbearbeiter die Daten auch effektiv vertrags- oder gesetzesgemäss bearbeitet, er kann jedoch dafür sorgen. **Zu Abs. 3:** Das Erfordernis der Schriftlichkeit erachten wir dann als zu einschränkend, wenn nicht auch die einfache elektronische Form miteingeschlossen ist. Im Erläuterungsbericht steht zwar geschrieben, dass die schriftliche Form die elektronische Form einschliesst. Es ist jedoch nicht so klar, was damit konkret gemeint ist Entspricht eine „einfache“ E-Mail diesen Vorgaben oder bedarf es z.B. der qualifizierten elektronischen Signatur? Die Hürde an die Schriftlichkeit darf nicht zu hoch sein und macht in diesem Zusammenhang auch keinen Sinn.

Art. 7 Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften entstehen.	~~**Art. 7 Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans**~~ ~~Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften entstehen.~~	**Zu Art. 7:** Die Bestimmung ist zu streichen, denn Art. 10 Abs. 2 lit. b revDSG enthält bereits die Verpflichtung an den Datenschutzberater bei der Anwendung des Datenschutzrechts mitzuwirken.
3. Abschnitt: Bekanntgabe von Personendaten ins Ausland		
Art. 8 Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs [1] Werden Personendaten ins Ausland bekanntgegeben, so müssen bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden: a. die internationalen Verpflichtungen des Staates oder internationalen Organs im Bereich des Datenschutzes; b. die Achtung der Menschenrechte; c. die geltende Gesetzgebung zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung; d. die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes; e. das wirksame Funktionieren von einer oder mehreren unabhängigen Behörden, die im betreffenden Staat mit dem Datenschutz beauftragt sind oder denen ein internationales Organ		

untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen. 2 Bei der Beurteilung können die Einschätzungen von internationalen Organen oder ausländischen Behörden, die für den Datenschutz zuständig sind, berücksichtigt werden. 3 Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch neu beurteilt. 4 Ergibt sich aus einer Beurteilung nach Absatz 3 oder aus verfügbaren Informationen, dass ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ kein angemessener Datenschutz mehr gewähr-leistet, so wird der Entscheid gemäss Artikel 16 Absatz 1 DSG geändert, sistiert oder aufgehoben. Dieser neue Entscheid hat keine Auswirkungen auf bereits erfolgte Datenbekanntgaben. 5 Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz sind in Anhang 1 aufgeführt. 6 Der EDÖB wird vor jedem Entscheid über die Angemessenheit des Datenschutzes konsultiert.		
Art. 9 Datenschutzklauseln und spezifische Garantien 1 Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen mindestens die folgenden Punkte regeln:		

a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung und der Richtigkeit; b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen; c. die Art und der Zweck der Bekanntgabe von Personendaten; d. die Namen der Staaten, in die Personendaten bekanntgegeben werden; e. die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden; f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten; g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger; h. die Massnahmen zur Gewährleistung der Datensicherheit; i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ; j. die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren; k. die Rechte der betroffenen Person, namentlich: 1. das Auskunftsrecht, 2. das Widerspruchsrecht, 3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten, 4. das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen. [2] Der Verantwortliche muss angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.		**Zu Abs. 1 lit. j:** Es ist unklar, weshalb der Datenempfänger die betroffenen Personen zu informieren hat. Eine solche Regelung ist als mit dem Tagesgeschäft nicht vereinbar. Diese Verpflichtung sollte beim Auftraggeber verbleiben. Es geht ja hier nicht um einen Auftragsbearbeiter nach Art. 9 revDGS. Weiter ist unklar, was „über die Bearbeitung informieren“ im Zusammenhang mit dem Empfänger bedeutet. Geht es lediglich darum zu melden, dass ein Dritter, nämlich der Empfänger, Daten der Person erhält, oder geht es um inhaltliche Informationen? Sofern lit. f beibehalten wird, ist dies hier zu präzisieren.

[3] Wurde der EDÖB über die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die: a. unter denselben Datenschutzklauseln oder Garantien erfolgen, soweit die Kategorien der Empfängerinnen und Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen Unternehmen, die zum selben Konzern gehören, stattfinden, soweit die Daten-schutzklauseln oder Garantien weiterhin einen geeigneten Datenschutz gewährleisten.		
Art. 10 Standarddatenschutzklauseln [1] Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet. [2] Der EDÖB veröffentlicht eine Liste von Standarddatenschutzklauseln, die er genehmigt, ausgestellt oder anerkannt hat.		**Zu Abs. 1:** Der Verantwortliche kann angemessene Massnahmen im Rahmen von vertraglichen Verpflichtungen treffen, um der Durchsetzung von Standarddatenschutzklauseln Nachhilfe zu verschaffen, er kann jedoch nicht gewährleisten und schon gar nicht sicherstellen, dass der Empfänger die entsprechenden Klauseln effektiv beachtet. Eine solche Verpflichtung ist nicht umsetzbar und mit Blick auf die hohen Strafbestimmungen nicht rechtens.
Art. 11 Verbindliche unternehmensinterne Datenschutzvorschriften [1] Verbindliche unternehmensinterne Datenschutzvorschriften nach Artikel 16 Absatz 2 Buchstabe e DSG gelten für alle Unternehmen, die zum selben Konzern gehören.		

[2] Sie umfassen mindestens die in Artikel 9 Absatz 1 genannten Punkte sowie die folgenden Angaben: a. die Organisation und die Kontaktdaten des Konzerns und seiner Unternehmen; b. die innerhalb des Konzerns getroffenen Massnahmen zur Gewährleistung der Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften.		
Art. 12 Verhaltenskodizes und Zertifizierungen [1] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn durch einen Verhaltenskodex oder eine Zertifizierung ein geeigneter Datenschutz gewährleistet wird. [2] Der Verhaltenskodex enthält mindestens die Angaben nach Artikel 9 Absatz 1 und muss vorgängig vom EDÖB genehmigt werden. [3] Der Verhaltenskodex oder die Zertifizierung muss mit einer verbindlichen und durchsetzbaren Verpflichtung des Verantwortlichen oder des Auftragsbearbeiters im Drittstaat verbunden werden, die darin enthaltenen Massnahmen anzuwenden.		
2. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters		
Art. 13 Modalitäten der Informationspflichten [1] Der Verantwortliche und der Auftragsbearbeiter teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit. [2] Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.		**Zu Art. 13:** In Art. 19 revDSG wird betreffend die Informationspflicht allein der Verantwortliche genannt. Hier soll nun plötzlich auch der Auftragsbearbeiter eine solche haben. Dies können wir nicht nachvollziehen. **Zu Abs. 2:** Wo besteht bei den Piktogrammen der Zusammenhang zu „maschinenlesbar“? Dies sollte noch im Detail erläutert werden.

Art. 14 Informationspflicht der Bundesorgane bei der systematischen Beschaffung von Personendaten Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin.		
Art. 15 Information bei der Bekanntgabe von Personendaten Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.		Vgl. unsere Bemerkungen zu Art. 13. Zudem fehlt hierzu unseres Erachtens eine Grundlage auf Gesetzesstufe. Eine solche Pflicht kann unseres Erachtens nicht allein auf Verordnungsstufe geregelt werden; dafür ist sie in der Umsetzung zu einschneidend.
Art. 16 Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten Der Verantwortliche informiert die Empfängerinnen und Empfänger, denen er Personendaten bekanntgegeben hat, unverzüglich über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten, ausser die Benachrichtigung ist unmöglich oder mit einem unverhältnismässigen Aufwand verbunden.	~~**Art. 16 Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten**~~ ~~Der Verantwortliche informiert die Empfängerinnen und Empfänger, denen er Personendaten bekanntgegeben hat, unverzüglich über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten, ausser die Benachrichtigung ist unmöglich oder mit einem unverhältnismässigen Aufwand verbunden.~~	**Zu Art. 16:** Diese Bestimmung wurde dazumal aus dem Vorentwurf des neuen DSG gestrichen (Art. 19 revDSG) und kann nicht auf dem Verordnungswege wieder eingefügt werden! Wie bereits in unserer Vernehmlassungsantwort zum revDSG festgehalten, geht diese Bestimmung zu weit und gilt als in der Praxis nicht umsetzbar.
Art. 17 Überprüfung einer automatisierten Einzelentscheidung Verlangt eine von einer automatisierten Einzelentscheidung betroffene Person, dass sie ihren Stand-		

punkt darlegen kann oder dass eine natürliche Person die Entscheidung überprüft, so darf sie deswegen nicht benachteiligt werden.		
Art. 18 Form und Aufbewahrung der Datenschutz-Folgenabschätzung Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.	.	Vgl. unsere Bemerkungen zu Art. 6 Abs. 3.
Art. 19 Meldung von Verletzungen der Datensicherheit 1 Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit: a. die Art der Verletzung; b. soweit möglich den Zeitpunkt und die Dauer; c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten; d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen; e. die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen; f. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Man-gel zu beheben oder die Folgen zu mildern; g. den Namen und die Kontaktdaten einer Ansprechperson. 2 Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.	2 Ist es dem Verantwortlichen **~~bei Entdeckung der Verletzung der Datensicherheit~~** nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.	**Zu Abs. 2:** Der Hinweis «bei Entdeckung der Verletzung der Datensicherheit» erscheint wenig sinnvoll. Zu diesem Zeitpunkt wird der Verantwortliche nie über alle Informationen verfügen, da sich diese immer erst über Zeit herausstellen. Der Hinweis kann ersatzlos gestrichen werden.

[3] Der Verantwortliche teilt den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mit. [4] Handelt es sich beim Verantwortlichen um ein Bundesorgan, so erfolgt die Meldung an den EDÖB über die Datenschutzberaterin oder den Datenschutzberater. [5] Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.		**Zu Abs. 5:** Es ist nicht nachvollziehbar (und mit den Grundsätzen des Datenschutzes unvereinbar), weshalb hier eine Aufbewahrungsdauer von drei Jahren gewählt wurde Diese Frist ist zu lang.
3. Kapitel: Rechte der betroffenen Person		
1. Abschnitt: Auskunftsrecht		
Art. 20 Modalitäten [1] Das Auskunftsbegehren wird schriftlich gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden. [2] Die Auskunft wird in der Regel schriftlich erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat. [3] Die Auskunft muss für die betroffene Person verständlich sein.		**Zu Abs. 1:** In welchen Sprachen müssen die Auskunftsbegehren beantwortet werden? Hat die Auskunft in x-beliebigen Sprachen zu erfolgen? Sinnvollerweise sollten Auskunftsbegehren in den Landessprachen sowie Englisch beantwortet werden können. In der Praxis stossen die Versicherer zudem immer wieder auf Schwierigkeiten betreffend Auskunft um Daten verstorbener Personen. Eine zusätzliche Regelung zum Umgang mit diesen Daten würden wir sehr begrüssen.

[4] Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken. [5] Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.	[4] Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken, **ansonsten die Auskunft verweigert werden darf.**	**Zu Abs. 4:** Für die Krankenversicherer ist es sehr wichtig, dass die Modalitäten der Auskunftserteilung korrekt erfolgen. Dabei bedarf es eben auch der Mitwirkung der betroffenen Personen. Zeigen sich diese nicht mitwirkungsbereit, haben sie die Konsequenzen entsprechend mitzutragen.
Art. 21 Zuständigkeit [1] Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter. [2] Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen.	**Art. 21 Zuständigkeit** [1] Sind für die Bearbeitung von Personendaten mehrere **gemeinsam** verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter. [2] Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, **sofern er das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet.**	**Zu Abs. 1:** Unklar ist, welche Rechtsfolge die «Unzuständigkeit» eines Verantwortlich hat. **Zu Abs. 2:** Diese Bestimmung ist verwirrlich, da sie impliziert, dass der Auftragsbearbeiter selbst eine Auskunftspflicht hat, wenn er faktisch in der Lage sein sollte, eine Auskunft zu erteilen bzw. er das Auskunftsgesuch in einem solchen Fall nicht weiterleiten muss, auch wenn er es nicht beantwortet. Das kann nicht sein. Die Regelung sollte präzisiert werden.
Art. 22 Frist [1] Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortli-		**Zu Art. 22:** Die Regelung sollte präzisiert werden. Die Frist kann erst dann zu laufen beginnen, wenn das Begehren klar und die betroffene Person korrekt identifiziert ist. Dies ist sie zu Beginn häufig nicht.

che die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen. 2 Kann die Auskunft nicht innert 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber benachrichtigen und ihr die Frist mitteilen, in der die Auskunft erfolgen wird.		
Art. 23 Ausnahmen von der Kostenlosigkeit 1 Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. 2 Die Beteiligung beträgt maximal 300 Franken. 3 Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen.		**Zu Abs. 1 und 2**: Eine maximale Kostenbeteiligung von CHF 300.00 deckt in keiner Art und Weise mögliche anfallenden Kosten der Krankenversicherer. Bereits heute schon sind die maximal CHF 300.00 in einzelnen Fällen viel zu tief in Bezug auf die tatsächlich anfallenden Kosten. Die maximale Kostenbeteiligung sollte mindestens bei CHF 2‘000.00 liegen (nur schon der Wertverfall alleine rechtfertigt eine Erhöhung von CHF 100.00). Weiter haben die allgemeinen Datenauskunftsbegehren in den letzten Jahren massiv zugenommen, nicht zuletzt auch, weil mit vorgefertigten Schreiben die Kunden zu entsprechenden Anfragen animiert werden. Ebenfalls nimmt auch die mit diesen Gesuchen verlangte Datenmenge zu. So sind sämtliche Daten aller Abteilungen innerhalb der Krankenversicherung herauszugeben oder zumindest deren Herausgabe von diversen Personen und Abteilungen zu prüfen. Der Aufwand ist beträchtlich und geht zulasten aller versicherten Personen! **Zu Abs. 3:** Sofern die Auskunft Kosten nach sich zieht, sollte die gesuchstellende Person verpflichtet werden, nochmals zu bestätigen, dass sie am Gesuch festhält. Ansonsten passiert es, dass der Krankenversicherer vergebens den enormen Aufwand auf sich nimmt und diesen nicht vergütet erhält. Wenn sich somit z.B. eine Person nicht mehr meldet, betreibt

		der Krankenversicherer so keinen unnötigen Aufwand. Zudem dient dies auch dem Schutz des Gesuchstellers, der ansonsten in Zugzwang gerät: Verpasst er die Frist, schuldet er (womöglich ungewollt) die Kostenbeteiligung.
2. Abschnitt: Recht auf Datenherausgabe oder -übertragung		
Art. 24 Die Artikel 20 Absätze 1, 4 und 5, sowie 21, 22 und 23 sind auf das Recht auf Datenherausgabe und -übertragung sowie deren Einschränkungen sinngemäss anwendbar.		
4. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch private Personen		
Art. 25 Datenschutzberaterin oder Datenschutzberater [1] Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen muss folgende Aufgaben wahrnehmen: a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden. b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will. [2] Der private Verantwortliche muss der Datenschutzberaterin oder dem Datenschutzberater: a. die notwendigen Ressourcen zur Verfügung stellen;	a. Sie oder er prüft die Bearbeitung von Personendaten ~~sowie deren Voraussetzungen~~ und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden.	**Zu Abs. 1 lit.a:** Den neuen Einschub «sowie deren Voraussetzungen» braucht es unseres Erachtens nicht. Wenn ein Datenschutzberater die Bearbeitung von Daten prüft, dann gehört die Prüfung der Voraussetzungen als logische Vorkontrolle grundsätzlich dazu und ist nicht explizit zu erwähnen. **Zu Abs. 2:** Bei der Bearbeitung durch die Privatperson fehlen in Analogie zu Art. 28 (Bearbeitung durch Bundesorgane) die wichtigen Ausführungen zur Unabhän-

b. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungs-tätigkeiten und Personendaten gewähren, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.		gigkeit und Weisungsungebundenheit des DS-Beraters, wie sie heute in Art. 12a und 12b VDSG ausgeführt sind. Man könnte ganz einfach diese hier übernehmen bzw. adaptieren.
Art. 26 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.		**Zu Art. 26:** Es ist unseres Erachtens klarzustellen, dass wenn eine der beiden Voraussetzungen erfüllt ist, die Verzeichnis-pflicht nur für die entsprechenden Bearbeitungen mit hohem Risiko gelten. Zudem sollte eine Übergangsfrist zur Umsetzung der Verzeichnispflicht von einem Jahr vorgesehen werden.
5. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane		
1. Abschnitt: Datenschutzberaterin oder -berater		
Art. 27 Ernennung Jedes Bundesorgan ernennt eine Datenschutzberaterin oder einen Datenschutzberater. Mehrere Bundesorgane können gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater ernennen.		
Art. 28 Anforderungen und Aufgaben [1] Die Datenschutzberaterin oder der Datenschutzberater muss die folgenden Anforderungen erfüllen:		**Zu Art. 28:** Gemäss Erläuterungsbericht kann der Datenschutzberater zwar grundsätzlich Empfehlungen aussprechen, aber die Entscheidungskompetenz liegt letztendlich beim Verantwortlichen. Somit liegt auch der Entscheid, ob eine Verletzung an den EDÖB gemeldet werden muss, beim Verantwortlichen. Wie ist

		nun die Situation, wenn der Verantwortliche aufgrund seiner Risikoabwägung keine Meldung vornehmen möchte – muss dann der Berater aufgrund seiner Verpflichtung gemäss Art. 28 Abs. 2 lit c revDSG die Verletzung dem EDÖB trotzdem melden? Und wer nimmt die Meldung vor, wenn eine private Person eine Verletzung melden muss, der Berater oder der Verantwortliche selbst? Und schliesslich - wer übernimmt künftig die Durchführung von datenschutzrechtlichen internen Audits? Dies gehört künftig gemäss revVDSG nicht mehr zum Aufgabenbereich des Datenschutzberaters, da nur noch beraten wird. Die Position des betrieblichen Datenschutzverantwortlichen, so wie wir ihn gegenwärtig kennen, wird zukünftig wohl generell beschnitten. Wenn man bedenkt, welche Aufgaben dieser gegenwärtig wahrnimmt, dann wird mit Einführung des revDSG und der revVDSG die Tätigkeit massiv eingeschränkt. Ist das sinnvoll und im Sinne der Revision?
a. Sie oder er verfügt über die erforderlichen Fachkenntnisse. b. Sie oder er übt ihre oder seine Funktion gegenüber dem Bundesorgan fachlich unabhängig und weisungsungebunden aus.		**Zu Abs. 1 lit. a:** Welche Fachkenntnisse müssen hier konkret erfüllt sein? Jus- oder Wirtschaftsabschluss, CAS Datenschutzberater? Oder reichen, wie bei vielen gegenwärtigen betrieblichen Datenschutzverantwortlichen, Berufserfahrung und gesunder Menschenverstand?
[2] Sie oder er muss folgende Aufgaben wahrnehmen: a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Vorausset-zungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden. b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese.		

c. Sie oder er meldet dem EDÖB Verletzungen der Datensicherheit. d. Sie oder er dient als Anlaufstelle für die betroffenen Personen. f. Sie oder er schult und berät das Bundesorgan sowie dessen Mitarbeiterinnen und Mitarbeiter in Fragen des Datenschutzes.	e. Sie oder er schult und berät das Bundesorgan sowie dessen Mitarbeiterinnen und Mitarbeiter in Fragen des Datenschutzes.	**Zu Abs. 2 lit. c:** Wie steht es mit all den anderen Datenschutzverstössen? Lit. c ist auf die „Datensicherheit" beschränkt. Verstösse wegen Unabhängigkeit sollen z.B. nicht gemeldet werden können? **Zu Abs. 2 lit. f:** Falsche Nummerierung. Es muss lit. e heissen.
Art. 29 Pflichten des Bundesorgans [1] Das Bundesorgan gewährt der Datenschutzberaterin oder dem Datenschutzberater Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt. [2] Es veröffentlicht die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters im Internet und teilt diese dem EDÖB mit.		
Art. 30 Anlaufstelle des EDÖB Die Datenschutzberaterin oder der Datenschutzberater dient dem EDÖB als Anlaufstelle für Fragen im Zusammenhang mit der Bearbeitung von Personendaten durch das betreffende Bundesorgan.		**Zu Art. 30:** Hier stellt sich uns die Frage, wie der Datenschutzberater künftig mit dem EDÖB zusammenarbeiten kann. Durch die einschneidende Kompetenzverengung vom betrieblichen Datenschutzverantwortlichen zum neuen Datenschutzberater dürfte es ihm künftig gar nicht mehr möglich sein, mit dem EDÖB ausführlich zu interagieren. Die gegenwärtige Unabhängigkeit wird durch seine „Beratertätigkeit" eingeschränkt.
2. Abschnitt: Projekte von Bundesorganen zur automatisierten Bearbeitung von Personendaten		
Art. 31 Information an die Datenschutzberaterin oder den Datenschutzberater		**Zu Art. 31:**

Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von Personendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden.		Hier bitten wir um eine Konkretisierung bezüglich den Begriffen „rechtzeitig“ und „sogleich“. Wir würden es begrüssen, wenn das Zeitfenster zwischen Abschluss des Projekts und der Implementierung der notwendigen datenschutzrechtlichen Mechanismen genauer definiert werden würde. Weiter fragt sich aus datenschutzrechtlicher Optik, weshalb diese Erfordernisse erst nach Abschluss des Projektes greifen und nicht bereits während des Projektes?
Art. 32 Meldung an den EDÖB [1] Das verantwortliche Bundesorgan meldet dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung. Der EDÖB nimmt diese Meldung in das Register der Bearbeitungstätigkeiten auf. [2] Die Meldung muss die Angaben nach Artikel 12 Absatz 2 Buchstaben a-d DSG sowie das voraussichtliche Datum des Beginns der Bearbeitungstätigkeiten enthalten. [3] Das verantwortliche Bundesorgan aktualisiert die Meldung beim Übergang in den produktiven Betrieb oder bei der Projekteinstellung.	~~**Art. 32 Meldung an den EDÖB**~~ ~~[1] Das verantwortliche Bundesorgan meldet dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung. Der EDÖB nimmt diese Meldung in das Register der Bearbeitungstätigkeiten auf.~~ ~~[2] Die Meldung muss die Angaben nach Artikel 12 Absatz 2 Buchstaben a-d DSG sowie das voraussichtliche Datum des Beginns der Bearbeitungstätigkeiten enthalten.~~ ~~[3] Das verantwortliche Bundesorgan aktualisiert die Meldung beim Übergang in den produktiven Betrieb oder bei der Projekteinstellung.~~	**Zu Art. 32:** Diese Anforderung entbehrt einer gesetzlichen Grundlage. Wenn es nur um die Planung der Ressourcen des EDÖB geht, rechtfertigt dies den Aufwand für den Krankenversicherer zudem nicht. Es ist kein Mehrwert ersichtlich. Weiter stehen bei Projektfreigabe viele Details zu den Bearbeitungen nicht fest, so dass eine Meldung mit den Angaben nach Art. 12 Abs. 2 lit. a-d revDSG nicht gemacht werden kann. Es braucht eine Präzisierung, wie beispielsweise die Bearbeitungstätigkeiten bei den Personendaten betroffen sind oder mit einem erhöhten Risiko einhergehen. Weiter enthält Art. 47 revDSG eine Übergangsbestimmung für automatisierte Bearbeitungstätigkeiten, die bei Inkrafttreten des revVDSG bereits produktiv sind. Diese Übergangsbestimmung ist keine Erleichterung, als für bereits produktive Bearbeitungen ein Verzeichnis erstellt und dieses an den EDÖB gemeldet werden muss.
3. Abschnitt: Pilotversuche		
Art. 33 Unentbehrlichkeit der Testphase Eine Testphase als Pilotversuch ist unentbehrlich, wenn eine der folgenden Bedingungen erfüllt ist:		

a. Die Erfüllung einer Aufgabe erfordert technische Neuerungen, deren Auswirkungen zunächst evaluiert werden müssen. b. Die Erfüllung einer Aufgabe erfordert bedeutende organisatorische oder technische Massnahmen, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit zwischen Organen des Bundes und der Kantone. c. Die Erfüllung der Aufgaben erfordert, dass die Personendaten mittels eines Abrufverfahrens zugänglich gemacht werden.		
Art. 34 Bewilligung [1] Vor der Konsultation der interessierten Verwaltungseinheiten legt das für den Pilotversuch zuständige Bundesorgan zu Handen des EDÖB dar, wie die Einhaltung der Anforderungen nach Artikel 35 DSG gewährleistet werden soll, und lädt ihn zur Stellungnahme ein. [2] Der EDÖB nimmt zur Frage Stellung, ob die Bewilligungsvoraussetzungen nach Artikel 35 DSG erfüllt sind. Das zuständige Bundesorgan stellt ihm alle dazu notwendigen Unterlagen zur Verfügung, insbesondere: a. eine allgemeine Beschreibung des Pilotversuchs; b. einen Bericht, der nachweist, dass die Erfüllung der gesetzlich vorgesehenen Aufgaben die Bearbeitung im Sinne von Artikel 34 Absatz 2 DSG erfordert und dass eine Testphase vor dem Inkrafttreten des Gesetzes im formellen Sinn unentbehrlich ist (Artikel 35 Absatz 1 Buchstabe c DSG); c. eine Beschreibung der internen Organisation sowie der Datenbearbeitungs- und Kontrollverfahren;		**Zu Art. 34:** Im Sinne der Planungssicherheit würden wir es begrüssen, wenn eine Frist definiert würde, innert welcher jeweils eine Stellungnahme des EDÖB erwartet werden darf.

d. eine Beschreibung der Sicherheits- und Datenschutzmassnahmen; e. den Entwurf einer Verordnung, welche die Einzelheiten der Bearbeitung regelt, oder das Konzept einer Verordnung; f. die Informationen betreffend die Planung der verschiedenen Phasen des Pilotversuches. 3 Der EDÖB kann weitere Dokumente anfordern und zusätzliche Abklärungen vornehmen. 4 Das zuständige Bundesorgan informiert den EDÖB über jede wichtige Änderung, welche die Einhaltung der Anforderungen von Artikel 35 DSG betrifft. Der EDÖB nimmt, falls erforderlich, erneut Stellung. 5 Die Stellungnahme des EDÖB ist dem Antrag an den Bundesrat beizufügen. 6 Die Modalitäten der automatisierten Datenbearbeitung werden in einer Verordnung geregelt.		
Art. 35 Evaluationsbericht Das zuständige Bundesorgan legt dem EDÖB den Entwurf des Evaluationsberichts an den Bundesrat zur Stellungnahme vor. Die Stellungnahme des EDÖB ist dem Bundesrat zur Kenntnis zu bringen.		Vgl. unsere Bemerkungen zu Art. 34
4. Abschnitt: Datenbearbeitung für nicht personenbezogene Zwecke		
Art. 36 Werden Personendaten zu nicht personenbezogenen Zwecken, insbesondere Forschung, Planung und Statistik, und gleichzeitig zu einem anderen Zweck bearbeitet, so sind die Ausnahmen nach Artikel 39 Absatz 2 DSG nur für die Bearbeitung zu		

den nicht personenbezogenen Zwecken anwendbar.		
6. Kapitel: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter		
Art. 37 Sitz und ständiges Sekretariat [1] Der Sitz des EDÖB befindet sich in Bern. [2] Auf die Arbeitsverhältnisse der Angestellten des ständigen Sekretariats des EDÖB ist die Bundespersonalgesetzgebung anwendbar. Die Angestellten des ständigen Sekretariats des EDÖB sind im Rahmen des Vorsorgewerks Bund bei der Pensions-kasse des Bundes PUBLICA gegen die wirtschaftlichen Folgen von Alter, Invalidität und Tod versichert.		
Art. 38 Kommunikationsweg [1] Der EDÖB verkehrt mit dem Bundesrat über die Bundeskanzlerin oder den Bundeskanzler. Diese oder dieser leitet die Vorschläge, Stellungnahmen und Berichte unverändert an den Bundesrat weiter. [2] Er reicht Berichte zuhanden der Bundesversammlung über die Parlamentsdienste ein.		
Art. 39 Mitteilung von Richtlinien und Entscheiden [1] Die Departemente und die Bundeskanzlei teilen dem EDÖB ihre Richtlinien im Bereich des Datenschutzes sowie ihre Entscheide in anonymisierter Form mit. [2] Die Bundesorgane legen dem EDÖB alle Rechtsetzungsentwürfe vor, welche die Bearbeitung von		

Personendaten, den Datenschutz sowie den Zugang zu amtlichen Dokumenten betreffen.		
Art. 40 Bearbeitung von Personendaten Der EDÖB bearbeitet Personendaten, einschliesslich besonders schützenswerter Personendaten, insbesondere zu folgenden Zwecken: a. zur Ausübung seiner Aufsichtstätigkeiten; b. zur Untersuchung von Verstössen gegen Datenschutzvorschriften; c. zur Schulung und Beratung von Bundesorganen und privaten Personen; d. zur Zusammenarbeit mit Bundesbehörden, kantonalen und ausländischen Behörden; e. zur Durchführung von Schlichtungsverfahren und Evaluationen nach dem Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (BGÖ); f. zur Beantwortung von Bürgeranfragen.		
Art. 41 Selbstkontrolle [1] Der EDÖB erstellt ein Bearbeitungsreglement für sämtliche automatisierten Bearbeitungen. Artikel 5 Absatz 1 findet keine Anwendung. [2] Er sieht interne Prozesse vor, die gewährleisten, dass die Bearbeitungen entsprechend dem Bearbeitungsreglement vorgenommen werden. Er überprüft jährlich, ob das Bearbeitungsreglement eingehalten wird.		**Zu Art. 41:** Der EDÖB sollte ebenfalls verpflichtet werden, zusätzlich ein Verzeichnis über sämtliche Bearbeitungstätigkeiten zu führen gemäss Art. 5 Abs. 1. Wir können nicht nachvollziehen, weshalb er davon befreit werden soll.
Art. 42 Zusammenarbeit mit dem Nationalen Zentrum für Cybersicherheit (NCSC) [1] Der EDÖB kann die Angaben zur Meldung einer Verletzung der Datensicherheit zwecks Analyse des Vorfalls dem NCSC weiterleiten. Der EDÖB muss		

vorgängig das Einverständnis des meldepflichtigen Verantwortlichen einholen. [2] Er lädt das NCSC zur Stellungnahme ein, bevor er gegenüber einem Bundesorgan eine Massnahme gemäss Artikel 51 Absatz 3 Buchstabe b DSG betreffend die Datensicherheit anordnet.		
Art. 43 Register der Bearbeitungstätigkeiten der Bundesorgane [1] Das Register der Bearbeitungstätigkeiten der Bundesorgane enthält die von den Bundesorganen und deren Auftragsbearbeiter gemachten Angaben nach Artikel 12 Absatz 2 und 3 DSG sowie Artikel 32 Absatz 2 dieser Verordnung. [2] Es ist im Internet zu veröffentlichen. Nicht veröffentlicht werden die Registereinträge über geplante automatisierte Bearbeitungstätigkeiten nach Artikel 32.		
Art. 44 Verhaltenskodizes Wird dem EDÖB ein Verhaltenskodex vorgelegt, so teilt dieser in seiner Stellungnahme mit, ob der Verhaltenskodex die Voraussetzungen nach Artikel 22 Absatz 5 Buchstabe a und b DSG erfüllt.		
Art. 45 Gebühren [1] Die vom EDÖB in Rechnung gestellten Gebühren bemessen sich nach dem Zeitaufwand. [2] Es gilt ein Stundenansatz von 150 bis 350 Franken. Dieser richtet sich nach der Komplexität des Geschäfts und nach der Funktion der für die Bearbeitung zuständigen Person.		**Zu Art. 45:** Bei der Erhebung von Gebühren besteht unseres Erachtens die Gefahr, dass Unternehmen nicht bereit sein werden, die Beratung oder andere Dienstleistungen des EDÖB in Anspruch zu nehmen. Dies könnte unter anderem dazu führen, dass Risiken oder Gefahren nicht entsprechend niedriger bewertet werden und dadurch die Datensicherheit nicht mehr gegeben ist.

[3] Im Übrigen gilt die Allgemeine Gebührenverordnung vom 8. September 2004.		
7. Kapitel: Schlussbestimmungen		
Art. 46 Aufhebung und Änderung anderer Erlasse Die Aufhebung und die Änderung anderer Erlasse werden im Anhang 2 geregelt.		
Art. 47 Übergangsbestimmung betreffend die Meldung geplanter automatisierter Bearbeitungstätigkeiten an den EDÖB Artikel 32 ist nicht anwendbar auf geplante automatisierte Bearbeitungstätigkeiten, bei welchen im Zeitpunkt des Inkrafttretens die Projektfreigabe oder der Entscheid zur Projektentwicklung bereits erfolgt ist.		
Art. 48 Inkrafttreten Diese Verordnung tritt am ... in Kraft.		**Zu Art. 48:** Da keine Übergangsfristen im Gesetz vorgesehen sind, muss das neue Recht (totalrevidiertes DSG samt Verordnung) bei dessen Inkrafttreten bereits vollständig implementiert sein. Für eine korrekte Umsetzung des neuen Rechts muss jedoch die definitive Fassung der Verordnung abgewartet werden. Diese wird wohl frühestens Ende 2021 vorliegen und der Öffentlichkeit zugänglich sein. Aktuell ist vom EJPD geplant, das neue Recht in der zweiten Hälfte 2022 in Kraft zu setzen, womit sich eine ausserordentlich kurze Umsetzungsfrist von einem halben Jahr ergeben würde. Das ist für die meisten Unternehmen nicht machbar. Die Inkraftsetzung sollte deshalb frühestens per 1. Januar 2023 erfolgen (je nach Entwicklungen später).

Vielen Dank für die Berücksichtigung unserer Anmerkungen. Für allfällige Fragen stehen wir gerne zur Verfügung.

Freundliche Grüsse

santésuisse

Direktion

Verena Nold
Direktorin santésuisse

Rechtsdienst

Isabel Kohler Muster
Leiterin Rechtsdienst santésuisse-Gruppe

From:	Verband
To:	Amstutz Jonas BJ
Subject:	Entwurf zur Totalrevision der Verordnung zum BG über den Datenschutz (VDSG) / Avant-projet Ordonnance relative à la loi fédérale sur la protection des données (OLPD) / Avamprogetto Ordinanza relativa alla legge federale sulla protezione dei dati (OLDP
Date:	Freitag, 25. Juni 2021 11:15:26
Attachments:	image001.png image002.png

Sehr geehrter Herr Amstutz

Wir danken Ihnen bestens für die Gelegenheit in eingangs erwähnter Sache Stellung nehmen zu können.

Da diese Vorlage gemäss Dossieraufteilung zwischen economiesuisse und dem Schweizerischen Arbeitgeberverband von economiesuisse bearbeitet wird, verzichten wir auf eine Stellungnahme zu dieser Vernehmlassung.

Ich wünsche Ihnen ein schönes Wochenende.

Freundliche Grüsse
Sabine Maeder

Assistentin
SCHWEIZERISCHER ARBEITGEBERVERBAND
Hegibachstrasse 47
Postfach
8032 Zürich
Tel. +41 44 421 17 17
Fax +41 44 421 17 18
Direktwahl: +41 44 421 17 42
maeder@arbeitgeber.ch
http://www.arbeitgeber.ch

Von: jonas.amstutz@bj.admin.ch <jonas.amstutz@bj.admin.ch>
Gesendet: Donnerstag, 24. Juni 2021 07:18
An: info@die-mitte.ch; info@edu-schweiz.ch; info@eag-ge.ch; vernehmlassungen@evppev.ch; info@fdp.ch; gruene@gruene.ch; schweiz@grunliberale.ch; lorenzo.quadri@mattino.ch; pdaz@pda.ch; gs@svp.ch; franziska.tlach@spschweiz.ch; verband@chgemeinden.ch; info@staedteverband.ch; info@sab.ch; info@economiesuisse.ch; bern@economiesuisse.ch; sandra.spieser@economiesuisse.ch; info@sgv-usam.ch; Verband <verband@arbeitgeber.ch>; info@sbv-usp.ch; office@sba.ch; info@sgb.ch; politik@kfmv.ch; info@travailsuisse.ch; direktion@bger.ch; behoerden@bvger.admin.ch; Info@bstger.ch; Kanzlei@bpatger.ch; beat.rudin@dsb.bs.ch; kommunikation@privatim.ch; info@vud.ch; info@frc.ch; mmarelli@icrc.org; info@redcross.ch; info@asci.ch; forum@konsum.ch; info@konsumentenschutz.ch; konsum@gs-wbf.admin.ch; office@digitale-gesellschaft.ch
Betreff: Entwurf zur Totalrevision der Verordnung zum BG über den Datenschutz (VDSG) / Avant-projet Ordonnance relative à la loi fédérale sur la protection des données (OLPD) / Avamprogetto Ordinanza relativa alla legge federale sulla protezione dei dati (OLDP)

Entwurf zur Totalrevision der Verordnung zum BG über den Datenschutz (VDSG): Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Damen und Herren

Am 23. Juni 2021 hat der Bundesrat das Vernehmlassungsverfahren zum Entwurf zur Totalrevision der Verordnung zum BG über den Datenschutz eröffnet. Beigefügt finden Sie das Orientierungsschreiben. Die Vernehmlassung dauert bis am 14. Oktober 2021.

Avant-projet de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) : ouverture de la procédure de consultation externe

Mesdames, Messieurs,

Le 23 juin 2021, le Conseil fédéral a ouvert la procédure de consultation concernant l'avant-projet de l'ordonnance relative à la loi fédérale sur la protection des données. Vous trouverez ci-joint la lettre d'information aux destinataires. La consultation est ouverte jusqu'au 14 octobre 2021.

Avamprogetto concernente l'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD): avvio della procedura di consultazione

Gentili Signore e Signori,

il 23 giugno 2021 il Consiglio federale ha avviato la consultazione sull'avamprogetto concernente l'ordinanza relativa alla legge federale sulla protezione dei dati.
In allegato trovate la lettera d'informazione ai destinatari. La consultazione dura fino al 14 ottobre 2021.

Freundliche Grüsse
Avec nos meilleures salutations,
Cordiali saluti

Jonas Amstutz
Sekretär

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik

Bundesrain 20, 3003 Bern
Tel. +41 58 467 86 65
jonas.amstutz@bj.admin.ch
www.bj.admin.ch

SAV FSA

Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

Eidgenössisches Justiz- und
Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Bundesrain 20
CHF-3003 Bern

Per Email versandt:
jonas.amstutz@bj.admin.ch

Bern, 14. Oktober 2021

Stellungnahme des Schweizerischen Anwaltsverbands SAV-FSA zum Vorentwurf der revidierten Verordnung zum Bundesgesetz über den Datenschutz (VE-VDSG)

Sehr geehrter Frau Bundesrätin,

Sehr geehrte Damen und Herren

Der Schweizerische Anwaltsverband (SAV) bedankt sich für die Einladung zur Vernehmlassung und nimmt dazu wie folgt Stellung:

Allgemeine Ausführungen

Der SAV begrüsst, dass die Revision des schweizerischen Datenschutzrechts mit der Vernehmlassung zum VE-VDSG ihre Fortsetzung findet. Der SAV erhofft sich insbesondere, dass mit der Revision die grenzüberschreitende Datenübermittlung zwischen der Schweiz und dem Europäischen Wirtschaftsraum weiterhin ohne zusätzliche Hürden möglich bleibt.

Der SAV verfolgt mit der vorliegenden Stellungnahme vor allem zwei Anliegen: Zum einen sind bei der Schaffung der neuen VDSG rechtsstaatliche und rechtspolitische Grundsätze einzuhalten. Zum anderen soll die neue VDSG für kleine und mittlere Unternehmen keine unverhältnismässigen Anforderungen aufstellen.

Der SAV stellt fest, dass sich der VE-VDSG in Teilen deutlich von den Vorgaben des neuen Datenschutzgesetzes (nDSG) entfernt hat. Die neue Verordnung (nVDSG) kann das nDSG nur dort konkretisieren, wo das nDSG eine solche Konkretisierung, das heisst entsprechende Ausführungsbestimmungen, vorsieht. Auf Konkretisierungen, die im nDSG nicht angelegt sind, muss der Verordnungsgeber aus rechtsstaatlichen Gründen verzichten, denn dafür fehlt die erforderliche gesetzliche Grundlage. Genauso muss der Verordnungsgeber aus rechtspolitischen Gründen auf Bestimmungen verzichten, die der Gesetzgeber in den parlamentarischen

Beratungen zum nDSG bewusst verworfen hat. Für solche überschiessenden Bestimmungen fehlt nicht nur der erforderliche Konsens, sie liefen auch dem gesetzgeberischen Willen zuwider.

Der SAV stellt weiter fest, dass der VE-VDSG zum Teil Anforderungen stellt, welche kleinste, kleine und mittlere Unternehmen als Verantwortliche kaum oder nur mit unverhältnismässigem Aufwand erfüllen können. Die meisten Anwältinnen und Anwälte sind in solchen kleinen oder mittleren wirtschaftlichen Strukturen tätig, wobei sie bereits einen erheblichen Aufwand für die Einhaltung der anwalts- und berufsrechtlichen Pflichten betreiben müssen. Dazu gehört insbesondere das Berufsgeheimnis, das in Bezug auf *alle* Daten von Mandantinnen und Mandanten bereits einen durchsetzbaren und wirksamen Datenschutz sicherstellt.

Der SAV stellt schliesslich fest, dass der VE-DSG überholte Elemente der geltenden VDSG unnötigerweise übernimmt und einen «Swiss Finish» gegenüber der europäischen Datenschutz-Grundverordnung (DSGVO) vorsieht. Auf solche Elemente wie auch auf einen «Swiss Finish» ist zu verzichten. Mit einem solchen Verzicht würden jene Verantwortlichen, die ergänzend zum nDSG die DSGVO umsetzen müssen oder bereits umgesetzt haben, nicht zusätzlich belastet. Für jene Verantwortlichen hingegen, die allein das nDSG umsetzen müssen, sollten Pflichten, die sich aus Konkretisierungen des nDSG in der nVDSG ergeben, insbesondere etwaige Dokumentationspflichten, erst nach einer Übergangsfrist von zwei Jahren gelten. Zur Vereinfachung der Einhaltung und Umsetzung sollten die Artikel in der nVDSG jeweils auf die zugrundeliegenden Artikel im nDSG verweisen.

Kommentar zu ausgewählten Artikeln

Art. 1 VE-VDSG

Abs. 1: Die Massnahmen sollten auf ihre Eignung hin beurteilt werden und nicht auf ihre Angemessenheit («angemessen» durch «geeignet» ersetzen).

Beim Kriterium der Implementierung sollte klargestellt werden, dass es nicht allein um Kosten, sondern auch um sonstigen Aufwand geht («Implementierungskosten» durch «Implementierungsaufwand» ersetzen).

Abs. 2: Die Überprüfung sollte «in angemessener Art und Weise» erfolgen, denn je nach Bearbeitung ist keine regelmässige Überprüfung erforderlich.

Art. 2 VE-VDSG

Der Katalog der Schutzziele sollte mit der Liste der Massnahmen gemäss Art. 32 DSGVO kompatibel sein, um die Umsetzung von nDSG *und* DSGVO zu erleichtern. Die Schutzziele sollten sich daher auf die Grundsätze der Vertraulichkeit, der Integrität und der Verfügbarkeit, die für die Datensicherheit im eigentlichen Sinne zentral sind, beschränken.

Art. 3 VE-VDSG

Der gesamte Artikel ist insbesondere mangels gesetzlicher Grundlage ersatzlos zu streichen. Er leidet zudem an systematischen Unstimmigkeiten (die Protokollierung ist keine Massnahme der Datensicherheit im eigentlichen Sinne) und fehlender Praktikabilität (der Auftragsbearbeiter weiss

nicht, ob eine Datenschutz-Folgenabschätzung durchgeführt wurde, und ohnehin ist die Datenschutz-Folgenabschätzung ein ungeeigneter Indikator für Risiken der Datensicherheit).

Art. 4 u. 5 VE-VDSG

Der gesamte Artikel 4 ist mangels gesetzlicher Grundlage und als «Swiss Finish» ersatzlos zu streichen. Eine so weitgehende Dokumentationspflicht widerspricht auch dem erklärten Willen des Gesetzgebers, weshalb auf eine allgemeine Dokumentationspflicht nach dem Muster der DSGVO zu verzichten ist. Ein solches Bearbeitungsreglement wäre im Übrigen unnötig (es ist bereits ein Bearbeitungsverzeichnis mit weitgehend deckungsgleichen Angaben zu führen) und unverhältnismässig. Das gilt genauso für Bundesorgane (Art. 5 VE-DSG).

Art. 6 VE-VDSG

Abs. 1: Der gesamte Absatz ist insbesondere mangels gesetzlicher Grundlage ersatzlos zu streichen. Es ist zudem unklar, was mit einer «vertrags- oder gesetzesgemäss[en]» Bearbeitung gemeint ist. Das Anliegen dürfte in Art. 9 Abs. 1 nDSG bereits abgedeckt sein.

Abs. 2: Der gesamte Absatz ist infolge abschliessender Regelung im nDSG ersatzlos zu streichen.

Art. 9 VE-VDSG

Abs. 1: Der Katalog der mindestens zu regelnden Punkte sollte als beispielhafte Aufzählung ausgestaltet werden, oder aber es ist klarzustellen, dass zu unterscheiden ist zwischen Verträgen, bei denen der Empfänger ein Verantwortlicher ist und solchen, bei denen er als Auftragsbearbeiter tätig wird.

Abs. 2: Es genügt, wenn der Verantwortliche in angemessener Art und Weise Sorge trägt, die Einhaltung sicherzustellen («Der Verantwortliche muss in angemessener Art und Weise Sorge tragen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die speziellen Garantien einhält»). Der Verantwortliche kann die Einhaltung nicht gewährleisten, er kann dafür nur in angemessener Art und Weise Sorge tragen.

Art. 10 VE-VDSG

Abs. 1: Es genügt, wenn der Verantwortliche in angemessener Art und Weise Sorge trägt, die Beachtung sicherzustellen («Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trägt er in angemessener Art und Weise dafür Sorge, dass die Empfängerin oder der Empfänger die Standarddatenschutzklauseln beachtet»).

Art. 13 VE-VDSG

Der gesamte Artikel ist mangels gesetzlicher Grundlage ersatzlos zu streichen. Offensichtlich falsch ist im Übrigen, dass auch der Auftragsbearbeiter eine Informationspflicht haben soll. Dies widerspricht nicht nur dem nDSG (Art. 19 nDSG verpflichtet richtigerweise nur den Verantwortlichen, nicht aber den Auftragsbearbeiter), sondern ist auch sachlich widersinnig.

Art. 15 VE-VDSG

Der gesamte Artikel ist mangels gesetzlicher Grundlage und als «Swiss Finish» ersatzlos zu streichen. Er ist zudem inhaltlich weder erforderlich noch praktikabel.

Art. 16 VE-VDSG

Der gesamte Artikel ist mangels gesetzlicher Grundlage ersatzlos zu streichen. Eine solche Informationspflicht hatte der Vorentwurf des nDSG noch vorgesehen. Der Gesetzgeber hat auf eine solche Pflicht indessen bewusst verzichtet. Sie kann daher nicht über die VDSG wieder eingeführt werden.

Art. 18 VE-VDSG

Satz 2 betreffend Aufbewahrungspflicht ist mangels gesetzlicher Grundlage ersatzlos zu streichen. Sie ist Teil einer umfassenden Dokumentationspflicht, die der VE-VDSG nun einführt, die dem Willen des Gesetzgebers aber widerspricht.

Art. 19 VE-VDSG

Abs. 5: Der gesamte Absatz ist mangels gesetzlicher Grundlage ersatzlos zu streichen. Er ist Teil einer umfassenden Dokumentationspflicht, die der VE-VDSG nun einführt, die dem Willen des Gesetzgebers aber widerspricht.

Art. 20 VE-VDSG

Abs. 3: Es genügt, wenn die Auskunft objektiv nachvollziehbar ist, auch wenn eine betroffene Person im Einzelfall nicht in der Lage sein mag, sie zu verstehen (Absatz vollständig durch «Die Auskunft muss nachvollziehbar sein» ersetzen).

Abs. 5: Der gesamte Absatz ist mangels gesetzlicher Grundlage ersatzlos zu streichen. Auch diese Bestimmung ist Teil einer umfassenden Dokumentationspflicht, die der VE-VDSG nun einführt, die dem Willen des Gesetzgebers aber widerspricht. Die Bestimmung ist zudem weder erforderlich noch praktikabel.

Art. 21 VE-VDSG

Abs. 1: Es sollte klargestellt werden, dass es um die gemeinsame Verantwortlichkeit geht («Sind für die Bearbeitung von Personendaten mehrere gemeinsam verantwortlich […]»).

Abs. 2: Bei einer Auftragsbearbeitung bleibt der auftraggebende Verantwortliche verantwortlich, das heisst, die Auskunft sollte immer durch den Verantwortlichen erteilt werden. Der gesamte Absatz ist deshalb ersatzlos zu streichen. Das entspricht auch der Regelung der DSGVO.

Art. 22 VE-VDSG

Abs. 1: Es sollte klargestellt werden, dass die Frist zur Erteilung des Auskunftsbegehrens erst beginnt, wenn die betroffene Person identifiziert ist und, sofern der Verantwortliche bei

umfangreicheren Begehren eine entsprechende Nachfrage stellt, wenn die betroffene Person ihr Begehren konkretisiert hat.

Art. 23 VE-VDSG

Abs. 2: Der gesamte Absatz ist ersatzlos zu streichen, da eine angemessene Beteiligung an den Kosten bereits in Abs. 1 enthalten ist. Die Beschränkung auf 300 Franken wäre je nach Aufwand für die Auskunftserteilung offensichtlich nicht angemessen.

Abs. 3: Es ist klarzustellen, dass die Frist zur Beantwortung erst beginnt, nachdem die betroffene Person über die Höhe der Kostenbeteiligung in Kenntnis gesetzt wurde.

Art. 25 VE-VDSG

Abs. 1: Der gesamte Absatz ist als überflüssig ersatzlos zu streichen, da Art. 10 nDSG bereits detaillierte Bestimmungen enthält.

Art. 26 VE-VDSG

Der Artikel lässt offen, für welche Bearbeitung ein Bearbeitungsverzeichnis zu führen ist, wenn nur eine der Voraussetzungen von lit. a und b erfüllt ist. Es sollte verdeutlich werden, dass die Pflicht jeweils nur für die Bearbeitung von Personendaten gilt, für die eine Voraussetzung nach lit. a oder b gilt, d.h. nur diejenigen Bearbeitungen, mit denen ein entsprechend erhöhtes Risiko einhergeht.

Der Begriff der «Mitarbeiterinnen und Mitarbeiter» soll durch «Vollzeitstellen» ersetzt werden, um Verantwortliche, die Teilzeitarbeit ermöglichen, nicht zu benachteiligen.

Es sollte eine Übergangsfrist von zwei Jahren für die Umsetzung vorgesehen werden.

Der Schweizerische Anwaltsverband dankt Ihnen für Ihre Kenntnisnahme.

Mit freundlichen Grüssen

Präsidentin SAV
Birgit Sambeth Glasner

Generalsekretär SAV
René Rall

SBB CFF FFS

Public Affairs und Regulation · Hilfikerstrasse 1 · CH-3000 Bern 65

Bundesamt für Justiz BJ
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Bern, 13. Oktober 2021

Vernehmlassung zur Revision der Datenschutzverordnung

Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, im Rahmen der Vernehmlassung über die Revision der Datenschutzverordnung (VDSG) Stellung nehmen zu können.

Die SBB ist Mitglied des Vereins Unternehmens-Datenschutz (VUD) und schliesst sich grundsätzlich vollumfänglich dessen Stellungnahme an. Wir möchten nachfolgend auf die besondere Betroffenheit konzessionierter Transportunternehmen (TU) fokussieren, die sich aus einer sektorspezifischen Bestimmung im Personenbeförderungsgesetz (PBG) ergibt.

Unternehmen als Bundesorgane

In der laufenden PBG-Revision geht der Bundesrat (vgl. BBl *2021* 1485) bei den mit der Personenbeförderung zusammenhängenden Datenbearbeitungen neu von öffentlich-rechtlichen Verhältnissen aus, weshalb für die SBB und alle weiteren TU die datenschutzrechtlichen Bestimmungen für Bundesorgane zur Anwendung gelangen würden. Dies hätte gewichtige Änderungen in den Prozessen des Personenverkehrs und damit des Kerngeschäfts der SBB zur Folge. Bisher sind die TU davon ausgegangen, dass die Personentransportverträge dem privaten Recht unterstehen und haben ihre Prozesse und Massnahmen diesbezüglich ausgestaltet. Das Urteil A-5921/2020 des Bundesverwaltungsgerichts vom 29. Juli 2021 hat den Personentransportvertrag und damit zusammenhängende Tätigkeiten der TU (der herrschenden Lehre entsprechend) als zivilrechtlich qualifiziert (E. 5.5). Unter dem Blickwinkel des Wertungswiderspruchs (E. 5.2.4) und unter Bezugnahme auf die vorgenannte PBG-Revision hat es eine Klärung empfohlen (E. 5.2.4). Der Geltungsbereich des nDSG und der VDSG hat insbesondere vor dem Hintergrund des geplanten Art. 54 PBG bei den TU grosse Unsicherheit ausgelöst.

SBB AG
Public Affairs und Regulation
Hilfikerstrasse 1 · 3000 Bern 65 · Schweiz
luca.arnold@sbb.ch / www.sbb.ch

Die SBB hat deshalb im Entwurf insbesondere die Bestimmungen für Bundesorgane geprüft. Die SBB möchte damit nicht Änderungen für «originäre» Bundesorgane wie Behörden der direkten Bundesverwaltung anregen. Vielmehr weist sie auf die besondere Betroffenheit der TU hin, da das PBG sie neu den öffentlich-rechtlichen Bestimmungen unterstellt. Datenbearbeitungen im ÖV basieren auf Kundenbeziehungen (Verträge) und stellen ein Massengeschäft dar. Die Tätigkeit eines TU ist nicht mit einem klassischen, hoheitlich handelnden Bundesorgan vergleichbar. Diesem Spannungsfeld trägt der Entwurf zu wenig Rechnung.

Einzelne Bestimmungen

Art. 3 Protokollierung
Die gesamte Vorschrift ist für TU problematisch, da einerseits die Protokollierung zu weit geht und unverhältnismässig ist und sie neu unter die strafbewehrte Datensicherheit fällt.

Art. 3 Abs. 2: Für die Protokollierungspflicht von sämtlichen automatisierten Bearbeitungen für Bundesorgane besteht keine Grundlage im DSG. Gemäss den Erläuterungen soll dazu die Richtlinie (EU) 2016/680 dienen. Die EU-Richtlinie bezweckt den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die *zuständigen* Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von *Straftaten* oder der *Strafvollstreckung*. Sie kann nicht als Grundlage für eine nicht risikoorientierte Protokollierungspflicht für TU und deren Bearbeitungen verwendet werden. Da die Datensicherheit gemäss Art. 8 nDSG risikoorientiert vorzunehmen ist, kann auch nicht eine umfassende Protokollierungspflicht in der Verordnung festgehalten werden und unter Art. 61 lit. c (Verletzung von Sorgfaltspflichten) fallen. Dazu reicht die gesetzliche Grundlage weder von Art. 8 nDSG noch aus der Richtlinie (EU) 2016/680 aus.

Weiter ist “automatisierte Bearbeitung” nicht definiert. Es ist somit davon auszugehen, dass jede mit einem technischen Hilfsmittel durchgeführte Bearbeitung darunter zu verstehen ist. Da Bundesorgane gemäss Entwurf nicht risikoorientiert handeln dürfen (im Gegensatz zu Privaten, Abs. 1) hätte das für die SBB folgende Konsequenzen:

Die SBB mit mehr als 33'000 Mitarbeitenden und gut 1 Mio. Passagieren pro Tag bearbeitet täglich eine unzählbare Anzahl Daten (z.B. Billettkontrollen). Der Aufwand und die Kosten für eine Protokollierung und Speicherung (vgl. Art. 3 Abs. 4) sämtlicher automatisierten Bearbeitungen im Bereich des Personenverkehrs sowie ihrer Auftragnehmer würde zu einer Datenflut führen. Die TU würden damit unverhältnismässig viele Daten speichern, was dem

datenschutzrechtlichen Verhältnismässigkeitsprinzip und auch den bisherigen Forderungen des EDÖB widerspricht.

Antrag: Die Protokollierungspflicht ist bei TU explizit auf die Bearbeitung besonders schützenswerter Personendaten und auf Profiling mit hohem Risiko zu beschränken. Die Protokollierungspflicht ist von der Strafbewehrung auszunehmen.

Art. 3 Abs. 4: Für die Aufbewahrungspflicht von 2 Jahren gibt es keine gesetzliche Grundlage. Das Datenschutzgesetz hat bewusst auf solche Dokumentationspflichten verzichtet. Zudem widerspricht die lange Speicherdauer dem Verhältnismässigkeitsprinzip.

Die Speicherung der Daten sämtlicher automatisierten Bearbeitungen (vgl. Ausführungen zu Art. 3 Abs. 2) würde unverhältnismässig hohe Kosten und Aufwand generieren. Eine getrennte Speicherung auf anderen Systemen würde bedingen, dass Kopien angefertigt und diese auf ein anderes und unabhängiges System übertragen werden müssen.

Antrag: Art. 3 Abs. 4 ist zu streichen. Die Speicherpflicht ist von der Strafbewehrung auszunehmen.

Art. 5 Bearbeitungsreglement von Bundesorganen
Die SBB ist daran, ein Datenbearbeitungsverzeichnis (DBV) einzuführen. Die Dokumentationspflichten sind über das vom DSG vorgegebene Verzeichnis der Bearbeitungstätigkeiten sichergestellt sowie über die Datenschutz-Folgenabschätzung. Das Verhältnis von DBV nach Art. 12 Abs. 1 nDSG und dem Bearbeitungsreglement gemäss Art. 5 ist unklar. Wir gehen aber davon aus, dass das Bearbeitungsreglement von Art. 5 keine eigenständige Bedeutung hat für TU, die ein DBV eingeführt haben. Wir beabsichtigen nicht, ein paralleles Bearbeitungsreglement zu führen.

Problematisch bleibt – wie bereits oben erwähnt -, was unter automatisierter Bearbeitung zu verstehen ist. Wenn damit alle nicht manuellen Bearbeitungen zu verstehen sind, führt die Dokumentationspflicht zu einer Detaillierungsstufe, die nicht zielführend und bewältigbar ist. Profiling ist auf ein hohes Risiko zu beschränken.

Antrag: Art. 5 ist für TU zu streichen. Eventualiter ist die Pflicht für TU, ein Bearbeitungsreglement zu führen, einzugrenzen: Statt jedes Profiling ist nur ein Profiling mit hohem Risiko zu dokumentieren. Die gesamte Bestimmung ist von der Strafbewehrung auszunehmen, da sie nicht die Datensicherheit im engeren und eigentlichen Sinn tangiert.

Art. 6 Modalitäten (Bearbeitung durch Auftragsbearbeiter)
Zu Abs. 3: Zu der Anforderung für TU, dass eine Subdelegation nur mit schriftlicher Erlaubnis des TU erfolgen darf, ist festzuhalten, dass eine allgemeine Genehmigung (entsprechend den Vorgaben der DSGVO[1]) zulässig ist und es keiner einzelfallbezogenen und spezifischen schriftlichen Einwilligungen bedarf. Diese Möglichkeit sehen Standard-Online-Services in ihren AGB nämlich nicht vor. Somit wäre es für TU nicht mehr möglich, solche Services zu beziehen. Nicht nur in den Erläuterungen sollte klargestellt werden, dass eine Genehmigung in Textform (z.B. E-Mail) den Anforderungen der Schriftlichkeit genügt.

Antrag: Klarstellung in der VDSG, dass eine Genehmigung in Textform genügt und sie auch in allgemeiner Form erfolgen kann (beides analog DSGVO).

Art. 7 Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans
Mit Art. 7 wird in die Organisationsfreiheit der TU eingegriffen, indem Vorgaben für rein interne Prozesse eines Unternehmens gemacht werden. Die SBB hat ca. 10'000 Rahmenverträge, welche meist auch datenschutzrechtliche Bestimmungen beinhalten. Der Einkauf ist für den Abschluss dieser Verträge zuständig. Die Datenschutzberater erstellen die Musterklauseln betreffend Datenschutz und beraten den Einkauf bei Verhandlungen, sofern notwendig. Eine nachträgliche Information über jeden abgeschlossenen Vertrag ist wirkungslos. Entscheidend ist, dass ein TU sicherstellt, dass die Verträge die Datenschutzvorschriften einhalten. Die Aufsicht über den Datenschutz durch den Datenschutzberater erfolgt risikobasiert bei den betreffenden Datenbearbeitungen und -auslagerungen und wird auch über die Datenschutz-Folgenabschätzungen gewährleistet.

Antrag: TU sind vom Anwendungsbereich von Art. 7 auszunehmen.

Art. 14 Informationspflicht der Bundesorgane bei der systematischen Beschaffung von Personendaten
Die Regelung ist für TU praxisfremd, denn es kann auch aus den Umständen hervorgehen, dass eine Auskunft freiwillig ist (z.B. bei jeder Kundenzufriedenheitsumfrage).

[1] Vgl. Art. 28 Abs. 2 Satz 2 DSGVO.

Antrag: Die Bestimmung ist zu ergänzen mit «soweit dies nicht aus den Umständen ersichtlich ist».

Art. 15 Information bei der Bekanntgabe von Personendaten
Die TU und Verbünde nutzen die Daten des öffentlichen Verkehrs gemeinsam. Der Datenaustausch ist im Übereinkommen Ue500 der Alliance SwissPass, welche vom Bundesamt für Verkehr (BAV) genehmigt wurde, geregelt. Diese Branchenregelung soll auch in Zukunft gelten.

In diesem Zusammenhang erlauben wir uns die Bemerkung, dass Richtlinie (EU) 2016/680 im Strafrechtsbereich gilt und nicht in anderen Bereichen als gesetzliche Grundlage verwendet werden kann.

Antrag: Die Bestimmung ist für TU zu streichen.

Art. 16 Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten
Auch bei Informationen über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten wenden die TU ihre eigenen Vorschriften an, vgl. Ausführungen zu Art. 15 oben. Im Übrigen weisen wir darauf hin, dass die Informationspflicht gemäss Art. 16 über keine gesetzliche Grundlage verfügt bzw. diese im Parlament gestrichen wurde. Die Vorgaben der Richtlinie (EU) 2016/680, die Schengener Zusammenarbeit im Strafrechtsbereich bezweckt, kann nicht als Grundlage dienen.

Ausserdem wird in der Bestimmung die «Einschränkung» der Bearbeitung erwähnt, welche so im Schweizer Datenschutzgesetz nicht existiert. Das nDSG kennt Einschränkungen der Informationspflicht (Art. 20 nDSG), des Auskunftsrechts (Art. 26 und 27 nDSG), der Datenherausgabe (Art. 29 nDSG) - nicht aber der Bearbeitung.

Antrag: Die Bestimmung ist für TU zu streichen.

Art. 27 Datenschutzberaterin oder -berater (Bundesorgane)
Für die SBB als TU ist zentral, dass die bisher für sie geltende Regelung beibehalten werden kann. Die SBB hat aufgrund ihrer Grösse mehr als einen Datenschutzberater. Bisher war sie deshalb von der Pflicht zur Meldung der Datensammlungen (neu Datenbearbeitungsverzeichnisse) befreit. Das soll für TU auch weiterhin gelten.

Antrag: Bei Bestellung eines Datenschutzberaters kommt für TU die Pflicht zur Anmeldung der Verzeichnisse (Art. 12 Abs. 4 nDSG) analog heutigem Recht (Art. 11a Abs. 5 lit. e DSG) nicht zur Anwendung.

Art. 31 Information an die Datenschutzberaterin oder den Datenschutzberater
Die Vorschrift macht rein interne Prozessvorgaben und greift somit unverhältnismässig in die Organisationsfreiheit von TU ein. Es muss dem verantwortlichen Unternehmen freistehen, wie es am besten mit seinen eigenen Prozessmethoden «privacy by design» umsetzen kann. Die SBB hat sich entsprechend organisiert. Wie ein interner Informationsfluss erfolgt, darf nicht in einer Verordnung geregelt werden.

Verschiedene Unternehmen kennen verschiedene Projektformen und operieren nicht zwingend nach der HERMES-Methode. Insbesondere die SBB führt ihre Projekte nicht mehr nach dem klassischen «Wasserfall-Modell» durch, sondern Anforderungen und entsprechende Projekte werden agil und fortlaufend erkannt und erarbeitet.

Antrag: TU sind von der Bestimmung auszunehmen.

Art. 32 Meldung an den EDÖB
Eine Pflicht, geplante Datensammlungen dem EDÖB zu melden, besteht für TU nach geltendem Recht nicht, sofern sie einen Datenschutzberater bestellt haben.

Die Meldepflicht jeder einzelnen nicht manuell durchgeführten Bearbeitung an den EDÖB generiert unverhältnismässig hohen Aufwand (auch für den EDÖB), ist nicht zielführend und widerspricht dem risikobasierten Ansatz des neuen Datenschutzgesetzes. TU, die einen Datenschutzberater stellen, sollten von der Meldepflicht an den EDÖB befreit sein.

Betreffend den Zeitpunkt der Meldung und die interne Projektorganisation wird grundsätzlich auf die Ausführungen zu Art. 31 des Entwurfs verwiesen: Eine Meldung im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung ist nicht mehr

praktikabel, da Projekte der SBB nicht mehr im klassischen «Wasserfall-Modell», sondern agil geplant und fortlaufend erarbeitet werden. Die Bestimmung verwendet damit Begriffe, die überholt sind, resp. so nicht mehr verwendet und nicht mehr gelebt werden. Zudem liegen die zu meldenden Informationen im Zeitpunkt, in dem die Meldung erfolgen soll, in der Regel nicht in der genügenden Detailtiefe vor. Die Ressourcenplanung des EDÖB rechtfertigt zudem nicht den mit dieser frühen Meldung einhergehenden Mehraufwand der Bundesbehörden.

Antrag: TU sind von der Bestimmung auszunehmen und können von der Konsultation des EDÖB im Zusammenhang mit Datenschutz-Folgenabschätzung absehen, wenn sie ihren Datenschutzberater konsultiert haben.

Art. 43 Register der Bearbeitungstätigkeiten der Bundesorgane
Es wird grundsätzlich auf die Ausführungen zu Art. 27 verwiesen. Zudem hat das Verzeichnis sämtlicher Datenbearbeitungen die Qualität eines Geschäftsgeheimnisses und kann nicht unbegrenzt der Öffentlichkeit zugänglich sein.

Antrag: TU, die einen Datenschutzberater bestellen, sind von der Meldepflicht der Datenbearbeitungen und ihres Verzeichnisses auszunehmen.

Wir bedanken uns für die Berücksichtigung unserer Anliegen. Die SBB ist bereit, diese mit den betroffenen Bundesämtern zu besprechen. In der Zwischenzeit steht Ihnen Anselm Filliger (anselm.filliger@sbb.ch) für Fragen zur Verfügung.

Freundliche Grüsse

i.V.

Stephanie Bregy
Leiterin Recht und Compliance

Luca Arnold
Leiter Regulation und Internationales

Kopie an: Gery Balmer, Abteilungschef Politik, Vizedirektor, BAV; Peter König, Sektionschef Recht, BAV

Swiss Banking

Frau Bundesrätin
Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Per Mail zugestellt an: jonas.amstutz@bj.admin.ch

Basel, 14. Oktober 2021
ABA / NGR +58 330 62 42

Stellungnahme zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 23. Juni 2021 eröffnete Vernehmlassung des Eidgenössischen Justiz- und Polizeidepartements zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG).

Wir bedanken uns bestens für die Konsultation in dieser für die Finanzbranche wichtigen Vernehmlassung. Gerne nehmen wir die Gelegenheit zur Stellungnahme wahr und unterbreiten Ihnen nachfolgend unsere Anliegen.

Die aus unserer Sicht wichtigsten Anliegen lauten wie folgt:

1. Der Entwurf der VDSG (E-VDSG) muss eine **reine Ausführungsverordnung** sein. Er enthält stattdessen zusätzliche Regelungen, welche über eine blosse Konkretisierung des revidierten Datenschutzgesetzes (nDSG) hinausgehen. Zahlreiche vorgeschlagene Regelungen setzen sich mit sehr strikten, regelbasierten Pflichten in Widerspruch zur übergeordneten, bewusst und konsequent prinzipien- und risikobasierten gesetzlichen Ordnung und produzieren damit sehr viel unnötigen Aufwand, oder gehen über das Niveau der Europäischen Datenschutzgrund-verordnung (EU-DSGVO) hinaus und schaffen dadurch unnötige, dem Regulierungsziel widersprechende und kontraproduktive "Swiss Finishes" zur EU-DSGVO (so z.B. Art. 2, Art. 3 Abs. 1, Art. 4 Abs. 1, Art. 6 Abs. 1 und 2, Art. 9, Art. 13 Abs. 1, Art. 15 bis 18, Art. 19 Abs. 5, Art. 20 Abs. 5, Art. 25 Abs. 1 Bst. b E-VDSG).
2. Entgegen den Regelungen auf Stufe des nDSG werden einzelne **Pflichten des Verantwortlichen gleichzeitig auch dem Auftragsdatenbearbeiter auferlegt**

(Art. 4 Abs. 1 und Art. 13 Abs. 1 E-VDSG) und setzen damit auch einen kontraproduktiven "Swiss Finish" zur EU-DSGVO.

3. Um eine faktische Aushöhlung der Feststellungskompetenz des Bundesrates sowie unterschiedliche Ergebnisse der Bewertung und eine damit einhergehende Rechtsunsicherheit zu vermeiden, muss ausdrücklich geregelt werden, dass die **Staatenliste des Bundesrates** (vgl. Art. 16 Abs. 1 nDSG und Art. 8 E-VDSG) für alle Akteure eine **verbindliche Feststellung zur Angemessenheit des Datenschutzes** darstellt.
4. Die **Pflicht zur Erstellung eines Bearbeitungsreglements** ist weitgehend deckungsgleich mit den Anforderungen an das neu gemäss Art. 12 nDSG zu erstellende Verzeichnis der Bearbeitungstätigkeiten, was **unnötigerweise Rechtsunsicherheit und unnötigen Doppelaufwand** produziert. Diese Pflicht ist deshalb zu streichen.

A. Einleitende Bemerkungen

1. "Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus (Art. 164 Abs. 2 BV). Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen (Art. 182 Abs. 2 BV). Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck (BGE 141 II 169 E 3.3)."

2. Viele im Rahmen der vorliegenden Vernehmlassung vorgeschlagenen Bestimmungen der E-VDSG verstossen offensichtlich gegen diese etablierten Rechtssetzungsgrundsätze, indem sie eindeutig über eine blosse Konkretisierung des revidierten Datenschutzgesetzes (nDSG) hinausgehen. Zahlreiche vorgeschlagene Regelungen setzen sich mit engmaschigen und starr regelbasierten Pflichten in Widerspruch zur übergeordneten, bewusst und konsequent prinzipien- und risikobasiert gestalteten gesetzlichen Ordnung und produzieren dadurch sehr viel unnötigen Aufwand, oder gehen über das Niveau der EU-DSGVO hinaus und schaffen dadurch unnötige, dem zentralen Regulierungsziel der EU-Äquivalenz widersprechende und damit kontraproduktive "Swiss Finishes" zur EU-DSGVO. Vielfach schränken die vorgeschlagenen Regelungen auch den vom Parlament entsprechend – auch im Bereich Datenschutz – bewährter schweizerischer Regulierung mit prinzipien- und risikobasierten Ansätzen bewusst offen gehaltenen Regelungsrahmen mit regelbasierten Anforderungskatalogen stark ein. Dadurch wird entgegen Systematik sowie Sinn und Zweck des nDSG verhindert, dass jeder Verantwortliche unter Anwendung vernünftigen Ermessens eine Umsetzung unter Würdigung seiner konkreten Verhältnisse vornehmen kann, namentlich entsprechend Grösse, Struktur, Komplexität, Risiken und Geschäftsmodell.

3. Dies ist im Bereich des Datenschutzes mit Blick auf die stark von KMU geprägte Struktur der schweizerischen Wirtschaft umso gravierender. Mehr als 99% sämtlicher Schweizer Unternehmen sind KMU mit weniger als 250 Mitarbeitenden, die meisten davon sogar Mikrounternehmen mit weniger als 10 Mitarbeitenden. Gleichzeitig stellen die KMU in der Schweiz rund zwei Drittel aller Arbeitsplätze. Viele KMU werden sich objektiv schlicht ausser Stande sehen, die umfangreichen im E-VDSG vorgeschlagenen Anforderungen mit vernünftigem Aufwand zu erfüllen bzw. mit Erfüllung sämtlicher Pflichten weiterhin ein gewinnbringendes Geschäftsmodell betreiben zu können. Dass zahlreiche datenschutzrechtliche Pflichten sogar mit strafrechtlichen Sanktionen bedroht sind (vgl. Art. 60 bis 64 nDSG), macht diesen Befund noch schlimmer.

4. Auch für die digitale Wirtschaft und damit für die Zukunftsfähigkeit und Innovationskraft des Wirtschaftsstandorts Schweiz ist ein gestützt auf vernünftiges Ermessen einfach umsetzbares Datenschutzgesetzgebungspaket notwendig. Der Bund fördert die Digitalisierung zu allen Aspekten und auf allen Stufen. Folgerichtig muss er es nicht zuletzt auch beim Thema Datenschutz tun.

5. Wegen den gesetzgeberischen Anliegen von Modernisierung und namentlich Annäherung an die EU-DSGVO ist das nDSG trotz bewusstem Erhalt seiner prinzipien- und risikobasierten Systematik gleichwohl deutlich länger als das bisherige DSG. Gerade die in Nachachtung der EU-DSGVO neu aufzunehmenden Themen waren im nDSG ausreichend deutlich darzustellen, um damit nicht zuletzt für die EU-Behörden im Hinblick auf deren Äquivalenzprüfung ausreichenden "Wiedererkennungswert" zu schaffen. Dies führt dazu, dass auf manche Präzisierung auf Verordnungsstufe gänzlich verzichtet werden sollte. Damit wird der gesetzgeberischen Idee des Parlaments entsprochen, den Verantwortlichen ausreichend vernünftiges Ermessen zu einer den konkreten Umständen angemessenen Umsetzung zur Verfügung zu stellen, namentlich entsprechend den Kriterien Grösse, Struktur, Komplexität, Risiken und Geschäftsmodell. Umso weniger ist sachlich nachvollziehbar, dass die E-VDSG tatsächlich sogar länger ausgefallen ist als die aktuell noch in Kraft befindliche VDSG.

6. Dem Parlament ist es gelungen, mit dem nDSG ein Gesetz zu schaffen, welches (a) einerseits den bewährten prinzipien- und risikobasierten Ansatz der schweizerischen Gesetzgebung auch im Bereich Datenschutz wahrt und (b) andererseits gleichzeitig mit gezielten Regeln zwecks Modernisierung und punktuellen Ergänzungen mit bewussten Annäherungen an die Regelungen der EU-DSGVO materielle EU-Äquivalenz zu schaffen. Dieses Resultat auf Gesetzesstufe wird durch die vorstehend skizzierte, verfehlte Systematik und Regelungsdichte der E-VDSG zunichte gemacht. Die typischerweise sehr strikten regelbasierten Verordnungsbestimmungen schränken den vom Parlament bewusst geschaffenen Umsetzungsspielraum massiv ein. In Anwendung einer Gesamtschau ergibt sich sogar, dass die unter Datenschutz in der Schweiz Verantwortlichen (a) einerseits sogar mit mehr formalen Regeln konfrontiert sind als im Anwendungsbereich der EU-DSGVO, und (b) wegen den von der E-VDSG vorgeschlagenen zahlreichen "Swiss Finishes" – entgegen der zielführenden Regelung – im nDSG die Aussicht auf Erhalt der EU-Äquivalenz abgesenkt wird.

7. Vorstehender Befund müsste sachlogisch eigentlich zu einer Rückweisung und Erarbeitung einer gänzlichen "Neuauflage" der E-VDSG führen. Dies nähme aber derart viel Zeit in Anspruch, dass dies wohl auch in zeitlicher Hinsicht die EU-Äquivalenz der Schweizer Datenschutzgesetzgebung gefährden würde und damit politisch nicht opportun erscheint. Deshalb verzichten wir bewusst auf einen solchen Rückweisungsantrag. Stattdessen legen wir Ihnen einen umfassenden Katalog mit notwendigen Anpassungen vor. Diese sind zwingend vorzunehmen, um die vorstehend aufgelisteten Negativbefunde nachhaltig zu korrigieren und damit ein Gesetzgebungspaket zu schaffen, welches die etablierten Regulierungsgrundsätze und die erklärten Regulierungsziele respektiert und die Wirtschaft entsprechend der gesetzgeberischen Absicht nicht mit unnötigem formalem Aufwand belastet.

Nachfolgend führen wir nun unsere Anpassungsanträge auf.

B. Detailkritik entlang der Systematik der E-VDSG

I. Datensicherheit

I.1. Art. 1 E-VDSG: Grundsätze

1. Sachlogische Anpassungen beim Begriff des "Risikos" (Art. 1 Abs. 1 Bst. b E-VDSG)

Ein Risiko ergibt sich sachlogisch vorab aus einer potenziellen Verletzung der Datensicherheit für die betroffene Person. Für den Fall des Vorliegens einer solchen potenziellen Verletzung stellt sich nachgelagert die Frage nach der Eintrittswahrscheinlichkeit. Dabei sind die Anforderungen an die Datensicherheit höher, je grösser die Eintrittswahrscheinlichkeit ist. Ohne potenzielle Datensicherheitsverletzung stellt sich umgekehrt die Frage nach der Eintrittswahrscheinlichkeit gar nicht. Die Formulierung in Art. 1 Abs. 1 Bst. b E-VDSG ist verwirrend, weil sie diese sachlogisch zwingende Reihenfolge nicht beachtet. Die Formulierung in Bst. b ist deshalb richtigerweise umzudrehen.

2. Berücksichtigung des Implementierungsaufwands statt der -kosten (Art. 1 Abs. 1 Bst. d E-VDSG)

Die Aufführung der Implementierungskosten als spezifisches Kriterium zur Beurteilung der Angemessenheit von technischen oder organisatorischen Massnahmen (sog. TOM) zur Gewährleistung der Datensicherheit ist nicht ausreichend. Neben eigentlichen Implementierungskosten fallen typischerweise auch weitere Aufwendungen an, welche zu berücksichtigen sind. Zu denken ist etwa an personelle, zeitliche und organisatorische Aufwendungen. Innerhalb einer Auswahl gleichwertiger angemessener Massnahmen darf der Verantwortliche die kostengünstigere auswählen. Dies ist aber selbstverständlich, ergibt sich dies doch bereits aus dem allgemeinen Verhältnismässigkeitsprinzip, und braucht deshalb nicht ausdrücklich erwähnt zu werden.

3. Anerkennung eines Umsetzungsermessens des Verantwortlichen (Art. 1 Abs. 2 E-VDSG)

Ob, wann und wie eine Überprüfung der TOM stattfinden soll, muss durch den Verantwortlichen selbst entschieden werden. Nur er ist in der Lage, den Besonderheiten des Einzelfalls hinreichend Rechnung zu tragen. Ist die Gefährdung der Rechte von Betroffenen grösser, so ist der zeitliche Abstand bis zur nächsten Prüfung sachlogisch kürzer. Die einseitige Fokussierung auf den zeitlichen Abstand einer Prüfung und die

zwingende Verknüpfung mit einer Prüfpflicht ist somit nicht sachgerecht, unnötig einengend und steht im Widerspruch zum risikobasierten Ansatz. Der Begriff "periodisch" ist deshalb zu streichen und "angemessene Abstände" durch "angemessene Weise" zu ersetzen.

Nach alledem müssen Art. 1 Abs. 1 Bst. b und d sowie Abs. 2 E-VDSG wie folgt angepasst werden:

Art. 1 E-VDSG

[1] Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:

a. Zweck, Art, Umfang und Umstände der Datenbearbeitung;
b. die ~~Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren~~ potenziellen Auswirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit (Restrisiko);
c. der Stand der Technik;
d. Implementierungsaufwand~~kosten~~.

[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen~~n~~r ~~Abständen~~Weise zu überprüfen.

I.2. Art. 2 E-VDSG: Schutzziele

Der Verordnungstext bringt zu wenig klar zum Ausdruck, dass sich die Notwendigkeit der in Art. 2 E-VDSG aufgeführten technischen und organisatorischen Massnahmen nach den in Art. 1 E-VDSG vorgeschriebenen Grundsätzen richtet.

Die in Art. 2 Abs. 2 E-VDSG aufgeführten Schutzziele sind zudem veraltet, zu absolut und zu detailliert geregelt. Entsprechend ihrer abstrakten Formulierung verleihen die Schutzziele zudem fälschlicherweise den Eindruck, dass es um absolut zu erreichende Anforderungen geht. Insofern werden statt Minimalanforderungen fälschlicherweise Maximalanforderungen formuliert. Dies ist nicht nur regulierungstechnisch verfehlt, sondern auch mit Blick auf die Strafbarkeit von Verletzungen der Datensicherheit (vgl. Art. 61 Bst. c nDSG). Die vorgeschlagene Regelung erfüllt einerseits nicht ansatzweise die strafrechtlichen Anforderungen an die Bestimmtheit der strafbaren Tat (Grundsatz "nulla poena sine lege"). Andererseits stünden gerade deshalb die meisten Verantwortlichen bzw. ihre Mitarbeitenden andauernd quasi "mit einem Bein im Gefängnis". Dies wiegt umso schwerer, als sehr viele Mitarbeitende eines Verantwortlichen im Zuge ihrer Arbeitstätigkeit tagtäglich naturgemäss Daten bearbeiten müssen und sich nicht – wie bei typischen Tätigkeitsdelikten wie z.B. der Veruntreuung – unter Würdigung der Strafandrohung und der weiteren Risiken – bewusst von der Tatbegehung Abstand nehmen können.

Im Kern muss es im – hier zu regelnden – Bereich der Datensicherheit um die Schutzziele Integrität, Verfügbarkeit, Vertraulichkeit und Belastbarkeit gehen. Eine generelle Dokumentationspflicht ist schon deshalb abzulehnen, weil diese so auch vom Gesetzgeber ausdrücklich abgelehnt worden ist.

Selbst die tatsächlich aufzuführenden Schutzziele Verfügbarkeit, Integrität, Verfügbarkeit und Belastbarkeit haben nur beispielhaften Charakter. Sie müssen namentlich dann nicht umgesetzt werden, wenn die Analyse nach Art. 1 E-VDSG dies nicht gebietet. Die Formulierung in der Verordnung sollte dies deutlich

zum Ausdruck bringen. Damit sollen nicht zuletzt auch KMUs (z.B. kleinere Banken) vor unnötigem administrativem Aufwand bewahrt werden.

Die vorgeschlagenen Formulierungen bringen zum Ausdruck, dass die Aufzählung in Art. 2 E-VDSG weder vollständig noch verpflichtend ist. Umgesetzt werden muss nur das, was nach Art. 1 E-VDSG zur Gewährleistung einer angemessenen Datensicherheit notwendig ist. Um dieses Ziel zu erreichen, können jedoch auch Massnahmen zur Anwendung kommen, die in Art. 2 E-VDSG nicht erwähnt sind. Mit den von uns beantragten Anpassungen ist die Liste auch konform mit den Anforderungen von Art. 32 EU-DSGVO. Ohne entsprechende Anpassungen läge demgegenüber ein kontraproduktiver "Swiss Finish" vor, welcher wegen unnötigen Zusatzaufwendungen und Zusatzrisiken auch die EU-Äquivalenz gefährden würde.

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.ch

Art. 2 E-VDSG

~~Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen~~Basierend auf den Grundsätzen nach Art. 1 ist insbesondere zu beurteilen, welche der nachfolgenden Schutzziele für Systeme und Dienste in Zusammenhang mit der Bearbeitung von Personendaten in Anwendung des risikobasierten Ansatzes im konkreten Fall anwendbar sind:

a. Vertraulichkeit:~~Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen.~~
b. Integrität;~~Zugangskontrolle: Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt.~~
c. Verfügbarkeit;~~Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht.~~
d. Belastbarkeit.~~Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert.~~
~~e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert.~~
~~f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.~~
~~g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden.~~
~~h. Bekanntgabekontrolle: Es kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden.~~
~~i. Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden.~~
~~j. Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).~~
~~k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.~~

Sollte diesem Antrag wider Erwarten nicht gefolgt werden, müssten die in der Liste gewählten Formulierungen zumindest so gewählt werden, dass sie nicht wie im Entwurf als absolut zu erreichende Maximalanforderungen daherkommen, sondern dass ihre Funktion als blosse Schutzziele, welche je nach Umständen mitzuberücksichtigen sind, klar zum Ausdruck gebracht werden.

I.3. Art. 3 E-VDSG: Protokollierung

Diese Bestimmung ist in dreierlei Hinsicht problematisch.

Das Parlament hat trotz detaillierter Formulierung der Anforderungen an die Datenschutzfolgeabschätzungen in Art. 22 nDSG bewusst auf eine Protokollierungspflicht verzichtet.

Darüber hinaus ergibt sich aus zahlreichen Voten im Parlament ebenso wie auch aus der finalen Fassung des nDSG mit aller wünschbaren Deutlichkeit, dass das Parlament am – auch ausserhalb des Datenschutzrechts – bewährten prinzipien- und risikobasierten Regulierungsansatz festhalten und – nicht zuletzt um unnötigen Aufwand für die zahlreichen KMU zu verhindern – namentlich auf unnötige Formvorschriften verzichten wollte. Dazu gehören neben strikte formulierten Dokumentations- und Protokollierungspflichten u.a. auch strikte Aufbewahrungsfristen (deren Dauer über die E-VDSG verteilt zudem eher zufällig mal kürzer, mal länger geregelt werden).

Die Festlegung der geeigneten organisatorischen und technischen Massnahmen zur Umsetzung von Pflichten gemäss nDSG muss in Anwendung des im nDSG – wie bisher – bewusst gewählten prinzipien- und risikobasierten Ansatzes jedem Verantwortlichen nach dessen vernünftigem Ermessen obliegen, namentlich entsprechend den Kriterien Grösse, Struktur, Komplexität, Risiken und Geschäftsmodell (vgl. schon oben Ziff. A.1-7).

Nach alledem widerspricht die in Art. 3 E-VDSG vorgeschlagene Protokollierungspflicht dem klaren gesetzgeberischen Willen und wäre überdies auch in seinen Wirkungen kontraproduktiv, würden doch in Anwendung dieser Pflicht umfassende Protokolle bzw. Logs über praktisch sämtliche Personendatenflüsse eines Verantwortlichen erstellt. Eine solche Pflicht auf Stufe E-VDSG wäre eine klare Verletzung des im nDSG verankerten Verhältnismässigkeitsprinzips (vgl. namentlich Art. 6 Abs. 2 und 3 nDSG), mithin dem wohl wichtigsten Grundprinzip für ein funktionierendes Datenschutzsystem. In Anwendung von Art. 3 E-VDSG würden denn auch statt Datenschutzprobleme zu lösen widersinnigerweise neue geschaffen.

Zusammengefasst fehlt es bei Art. 3 E-VDSG an einer gesetzlichen Grundlage. Zudem ist die Regelung nicht geeignet, das regulatorische Ziel zu erreichen. Schliesslich zielt die Regelung an der Sache vorbei und produziert lediglich unnötigen Zusatzaufwand, ohne den Datenschutz zu verbessern. Im Gegenteil schafft die Regelung unnötigerweise sogar neue Datenschutzprobleme und ist damit kontraproduktiv.

Nach alledem ist Art. 3 E-VDSG konsequenterweise ersatzlos zu streichen.

~~**Art. 3 E-VDSG**~~

~~[1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.~~

~~[2] Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.~~

~~[3] Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.~~

~~[4] Die Protokolle sind während zwei Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvor-schriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.~~

Will man wider Erwarten nicht so weit gehen, müsste nach dem Gesagten im Titel und in den Absätzen 1-3 zumindest die Anforderung "Protokollierung" durch "angemessene Dokumentation" ersetzt werden, sowie in Absatz 4 "Die Protokolle sind während zwei Jahren […] aufzubewahren." durch: "Die Aufbewahrungsfrist muss, sofern eine solche gesetzlich festgelegt ist, abhängig von Dauer und Datenbearbeitung und generell angemessen sein".

I.4. Art. 4 E-VDSG: Bearbeitungsreglement von privaten Personen

Die Regelung wurde im Wesentlichen aus Art. 11 der geltenden VDSG übernommen. Schon jene Bestimmung blieb aber insofern "toter Buchstabe", als es ein solches "Bearbeitungsreglement" in dieser Form in der operativen Praxis von Unternehmen nicht gibt. Vielmehr werden die zahlreichen notwendigen Regelungen gemäss bewährter Usanz in einem ganzen Paket von sich gegenseitig ergänzenden Weisungen samt dazugehörigen Prozessen und Listen mit Aufgaben, Kompetenzträgern und Verantwortlichkeiten abgebildet. Diese sind sehr viel wirkungsvoller als ein starres Reglement.

Die Regelung von Art. 4 E-VDSG ist zudem weitgehend deckungsgleich mit den neuen im nDSG eingeführten Informations- und Dokumentationspflichten, namentlich in direktem Zusammenhang mit Datenschutzfolgeabschätzungen gemäss Art. 22 nDSG und überdies mit den Anforderungen an das gemäss Art. 12 nDSG zu erstellende Verzeichnis der Bearbeitungstätigkeiten. Unter Würdigung dieses neuen Pakets von Anforderungen bereits auf Stufe nDSG erscheint das Festhalten am bisher schon als wenig hilfreich

kritisierten Bearbeitungsreglement gänzlich unnötig. Es würde lediglich unnötigerweise Rechtsunsicherheit und unnötigen Doppelaufwand ohne Mehrwert produzieren.

Die Aufgreifkriterien gemäss Art. 4 Abs. 1 E-VDSG sind keineswegs klar abgrenzbar. Im Bereich Profiling besteht unter Würdigung sämtlicher Kriterien ein gewisses Ermessen, wann die Grenze zu "hohem Risiko" erreicht ist. Die gesetzliche Regelung (vgl. Art. 5 Bst. f und g nDSG) gibt hiezu auch keine klaren Vorgaben, weil nur technische Beschreibungen ohne echte Abgrenzungskriterien festgelegt wurden. Namentlich wiederholt die Regelung für Profiling mit hohem Risiko (Art. 5 Bst. g nDSG) im Kern einen technischen Beschrieb, welcher auf jedes Profiling zutrifft und lässt offen, welches die Grenze zu "hohem Risiko" ist. Kritisch ist auch das Aufgreifkriterium "Bearbeitung umfangreicher besonders schützenswerter Personendaten" gemäss Art. 4 Abs. 1 Bst. a E-VDSG. Dies dürfte bei HR-Daten relativ rasch der Fall sein, auch bei KMU. Die offene Formulierung "umfangreich" ist deshalb als Aufgreifkriterium nicht geeignet. Nach alledem müssten sorgfältige Verantwortliche im Zweifelsfall einen Grossteil ihrer Datenbearbeitungen den Regeln von Art. 4 E-VDSG unterstellen. Gemäss Systematik von Art. 4 Abs. 1 E-VDSG ist dies aber gar nicht beabsichtigt, soll doch Art. 4 E-VDSG nur auf Ausnahmen von der Regel anwendbar sein. Diese gänzlich misslungene Regelung ist ein eigenständiger Grund für die ersatzlose Streichung von Art. 4 E-VDSG.

Ein solches Bearbeitungsreglement ist denn auch in der EU-DSGVO nicht vorgesehen und stellt somit in der E-VDSG einen kontraproduktiven "Swiss Finish" dar.

Kommt dazu, dass Art. 4 E-VDSG entgegen der systematischen Einordnung offensichtlich nicht Themen der Datensicherheit regelt, sondern vielmehr die Einhaltung von Bearbeitungsgrundsätzen.

Die Regelung von Art. 4 E-VDSG generiert somit statt Klärung bloss Verwirrung und unnötige Abgrenzungsprobleme und verkehrt entgegen erklärter Absicht das System von Regel und Ausnahme ins Gegenteil. Zudem ist es gänzlich sinnlos, weitgehend deckungsgleiche Regelungen zu erlassen. Dies umso mehr, als die meisten Schweizer Unternehmen überdies auch grenzüberschreitende Geschäfte betreiben und deshalb entsprechende Verzeichnisse nicht nur nach dem nDSG, sondern überdies auch nach der EU-DSGVO erarbeiten müssen. Demzufolge ist Art. 4 E-VDSG gar nicht nötig und ersatzlos zu streichen.

Die gesamte Regelung von Art. 4 Abs. 1 bis 3 E-VDSG ist somit ersatzlos zu streichen.

~~Art. 4 E-VDSG~~

~~[1] Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie:~~

~~a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder~~

~~b. ein Profiling mit hohem Risiko durchführen.~~

~~[2] Das Reglement muss mindestens Angaben enthalten:~~

~~a. zum Bearbeitungszweck;~~

~~b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;~~

~~c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;~~

~~d. zur internen Organisation;~~

~~e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung;~~

~~f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit;~~

~~g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe;~~

~~h. zu den Massnahmen, die zur Datenminimierung getroffen werden;~~

~~i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung;~~

~~j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.~~

~~[3] Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.~~

Falls an der Pflicht zur Erstellung eines Bearbeitungsreglements wider Erwarten festgehalten werden sollte, müsste zumindest der Auftragsbearbeiter in Art. 4 Abs. 1 E-VDSG gestrichen werden, da dessen Erwähnung der gesetzlichen Regelung im nDSG widerspricht (vgl. Art. 9 nDSG; vgl. unten Ziff. IV.1). Zudem sollten die Angaben in Art. 4 Abs. 2 E-VDSG jedenfalls nicht über jene in Art. 12 Abs. 2 nDSG hinausgehen und Art. 4 Abs. 3 E-VDSG – mangels einer Pflicht eines privaten Verantwortlichen zur Bestellung einer Datenschutzberaterin oder eines Datenschutzberaters – gestrichen werden.

Folglich wäre Art. 4 E-VDSG – **eventualiter** – wie folgt anzupassen:

Art. 4 E-VDSG

[1] Der Verantwortliche ~~und dessen Auftragsbearbeiter müssen~~muss ein Reglement für automatisierte Bearbeitungen erstellen, wenn ~~sie~~er:

a. umfangreich besonders schützenswerte Personendaten bearbeitetn; oder

b. ein Profiling mit hohem Risiko durchführten.

[2] Das Reglement muss mindestens Angaben enthalten:

a. zum Bearbeitungszweck;

b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;

c. wenn möglich zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;

~~d. zur internen Organisation;~~

~~e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung;~~

f. ~~zu den technischen und organisatorischen~~wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Art. 2.~~;~~

~~g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe;~~

~~h. zu den Massnahmen, die zur Datenminimierung getroffen werden;~~

~~i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung;~~

~~j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.~~

~~[3] Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.~~

II. Bearbeitung durch Auftragsbearbeiter

II.1. Art. 6 Abs. 1 E-VDSG: Modalitäten

Der erste Satz wiederholt einerseits eine Banalität, ist andererseits aber ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall eingeschränkt ist, auch dann, wenn ihm nichts vorgeworfen werden kann. Dem ist nicht so. Es ist ohnehin nicht klar, was mit "für den Datenschutz verantwortlich" gemeint ist. Strafrechtliche Verantwortlichkeit kann es nicht sein, und aufsichtsrechtliche Verantwortlichkeit setzt ebenfalls Kontrollmöglichkeiten voraus. Wird die Verantwortlichkeit schliesslich als zivilrechtliche Haftung verstanden, dann wird mit dieser Regelung eine vom Gesetzgeber nicht vorgesehene Kausalhaftung eingeführt. Hierfür fehlt klarerweise eine gesetzliche Grundlage. Dies würde auch über Art. 82 Abs. 3 EU-DSGVO hinausgehen. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR.

Zudem ist die Formulierung "sicherstellen" inhaltlich falsch. Der Verantwortliche kann nur "dafür Sorge tragen".

Auch der zweite Satz ist mangelhaft, da ihm ebenfalls eine gesetzliche Grundlage fehlt. Nach Art. 9 Abs. 1 Bst. a nDSG hat der Verantwortliche dafür zu sorgen, dass die Daten so bearbeitet werden, wie er es selbst darf. Nach Satz 2 hat er jedoch auch für die Durchsetzung seines eigenen Vertrags zu sorgen, selbst wenn dieser strenger sein sollte als das Gesetz. Macht er also einen zu strengen Vertrag, erlaubt aber seinem Auftragsbearbeiter eine Bearbeitung, die noch dem Gesetz entspricht, ist diese Vorschrift bereits verletzt. Die Regel verwirrt also mehr als sie nutzt. Schon nach Art. 9 Abs. 1 Bst. a nDSG hat der Verantwortliche dafür zu sorgen, dass das DSG eingehalten wird. Das genügt.

Aufgrund der obigen Ausführungen ist Art. 6 Abs. 1 E-VDSG ersatzlos zu streichen.

~~**Art. 6 Abs. 1 E-VDSG**~~

~~[1] Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.~~

[…]

II.2. Art 6 Abs. 2 E-VDSG: Modalitäten

Der Sinn und Zweck dieser Regelung erschliesst sich nicht, da der Regelungsgehalt bereits durch die Art. 16 und 17 nDSG (Bekanntgabe von Personendaten ins Ausland) abgedeckt ist. Gemäss Erläuterungsbericht entspricht der neue Art. 6 Abs. 2 E-VDSG dem geltenden Art. 22 Abs. 3 VDSG. Dabei handelt es sich aber um eine Bestimmung für Bundesorgane, während Art. 6 Abs. 2 E-VDSG sowohl für Datenbearbeitungen Privater als auch für solche von Bundesorganen gelten soll. Aus dem Erläuterungsbericht geht nicht hervor, warum diese Bestimmung nun auch für Private gelten soll. Offen bleibt auch, weshalb es die Regelung überhaupt braucht bzw. auf welche Rechtsgrundlage sie sich stützt.

Die Regelung würde nur dort halbwegs Sinn machen, wo ein Schweizer Verantwortlicher einen ausländischen Auftragsbearbeiter einsetzt, um Daten zu bearbeiten, ohne dass es zu einer Bekanntgabe

aus der Schweiz kommt und somit Art. 16 nDSG nicht greift. Systematisch wäre aber auch dieser Fall in Art. 16 nDSG zu regeln und nicht in der VDSG. Zudem ist diese Konstellation ein absolut "exotischer" Sonderfall. Eine eigene Regelung in der E-VDSG rechtfechtfertigt sich somit nicht. Die Regelung ergibt sich im Übrigen ohnehin bereits aus Art. 9 Abs. 1 Bst. a nDSG, und zwar systematisch korrekt, während sie hier systematisch falsch angelegt ist: Im Falle einer Auftragsbearbeitung geht es um die Sicherstellung eines gleichwertigen Datenschutzes, da der Auftragsbearbeiter die Daten gar nicht in eigener Regie bearbeiten darf. Vielmehr geht es darum sicherzustellen, dass die Daten nur so bearbeitet werden, wie der Verantwortliche dies darf – und so steht es schon in Art. 9 Abs. 1 Bst. a nDSG.

Es ist allerdings zweifelhaft, ob die Autoren der Regelung diesen Sonderfall überhaupt im Blick hatten. Vermutlich wurde die Regel einfach übernommen, weil es sie schon gab.

Aufgrund obiger Ausführungen ist Art. 6 Abs. 2 E-VDSG ersatzlos zu streichen.

~~Art. 6 Abs. 2 E-VDSG~~

[…]

~~[2] Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.~~

III. Bekanntgabe von Personendaten ins Ausland

III.1. Art. 8 E-VDSG: Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs: Zuständigkeit des Bundesrats

1. Irreführender Wortlaut (Art. 8 Abs. 1 und 6 E-VDSG)

Nach Art. 16 Abs. 1 nDSG legt nunmehr der Bundesrat fest, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten.

Der Wortlaut von Art. 8 Abs. 1 und 6 E-VDSG kann entgegen dieser Rechtslage gemäss nDSG dahingehend missverstanden werden, dass die verantwortliche Stelle – und nicht der Bundesrat – die Angemessenheit des Datenschutzes in einem Empfängerstaat feststellen muss.

Daher ist in Absatz 1 als auch in Absatz 6 eine entsprechende Klarstellung einzufügen.

Art. 8 Abs. 1 und 6 E-VDSG

[1] Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen~~t werden~~:

a. die internationalen Verpflichtungen des Staates oder internationalen Organs im Bereich des Datenschutzes;
b. die Achtung der Menschenrechte;
c. die geltende Gesetzgebung zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung;
d. die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes;
e. das wirksame Funktionieren von einer oder mehreren unabhängigen Behörden, die im betreffenden Staat mit dem Datenschutz beauftragt sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen.

[…]

[6] Der Bundesrat konsultiert den EDÖB ~~wird~~ vor jedem Entscheid über die Angemessenheit des Datenschutzes ~~konsultiert~~.

2. Implikationen als Folge der Rechtsprechung des Europäischen Gerichtshofs (EuGH) in der Rechtssache Schrems II sowie des Positionspapiers und der Handlungsanleitung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in gleicher Sache (Art. 8 Abs. 1 Satz 2 E-VDSG und Abs. 7 E-VDSG)

2.1. Allgemeine Einführung

Wie bereits erwähnt, legt nunmehr der Bundesrat fest, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten. Gemäss dem Erläuternden Bericht des Bundesamtes für Justiz soll daher die Verordnung neu die Kriterien regeln, welche der Bundesrat bei seinem Entscheid berücksichtigt. In Anhang 1 sind tabellarisch diejenigen Staaten und internationalen Organe aufgeführt, welche über ein angemessenes Datenschutzniveau verfügen.

Der Bundesrat erstellt die Liste der Länder mit angemessenem Datenschutz nach bestem Wissen und Gewissen. Die Verantwortlichen dürfen sich zwar im Prinzip auf diese Liste verlassen und müssen mithin nicht per se eigene Abklärungen vornehmen, welche die Einschätzung des Bundesrates bestätigen. Die Liste geniesst aber keinen öffentlichen Glauben (anders als z.B. das Grundbuch). Die Verantwortlichen dürfen sich deshalb nur, aber immerhin solange auf Gutgläubigkeit berufen und sich auf die Liste verlassen, wie ihnen aus eigener Praxiserfahrung nichts Gegenteiliges bekannt ist. Ohne dahingehenden eigenständigen Verdachtsanlass selbst Abklärungen über die Richtigkeit der Liste vornehmen, muss der Verantwortliche aber nicht (vgl. schon die Erläuterungen des Bundesamtes für Justiz zum DSG vom 24. März 2006, S. 8, Antwort zu Frage 49).

Am 18. Juni 2021 hat der EDÖB eine Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug veröffentlicht. Soweit danach ein Land auf der Staatenliste (des EDÖB und künftig des Bundesrates) fehlt oder mit einem ungenügenden Schutzniveau ausgewiesen ist, muss der Datenexporteur prüfen, ob kumulativ folgende vier Garantien eingehalten werden:

- klare Rechtsgrundlage betreffend Zwecke sowie Verfahren und materiellrechtliche Voraussetzungen des behördlichen Datenzugriffs und Befugnisse der Behörden;
- Verhältnismässigkeit der behördlichen Befugnisse und Massnahmen;
- wirksame gesetzlich verankerte Rechtsbehelfe für die Durchsetzung von Rechten von Betroffenen in der Schweiz;
- Rechtsweggarantie und Zugang zu einem unabhängigen und unparteiischen Gericht.

Erfüllt das lokale Recht die genannten Garantien nicht, muss der Datenexporteur weitere technische, organisatorische und rechtliche Massahmen treffen. Kann durch solche Massnahmen der fehlende Schutz nicht ausgeglichen werden, muss die Datenbekanntgabe ins Ausland ausgesetzt bzw. beendet werden.

Nach der Handlungsanleitung des EDÖB soll der Datenexporteur als gutgläubig gemäss Art. 3 Abs. 1 ZGB gelten, soweit er Daten in einen Staat übermittelt, der auf der Staatenliste als ein solcher mit angemessenem Datenschutzniveau aufgeführt wird. Hierbei soll es sich allerdings um eine widerlegbare Vermutung handeln. So soll der verantwortliche Datenexporteur bei der Erfassung und Analyse des Datentransfers alle nötigen Abklärungen vornehmen müssen, wie z.B. Einholen von unabhängigen Rechtsgutachten, u.a. zu folgenden Aspekten:

- Geltende Rechtsvorschriften im Zielland;
- Praxis der Verwaltungsbehörden und Gerichtsbehörden;

- Rechtsprechung.

2.2 Verbindlichkeit des Entscheids des Bundesrats zur Angemessenheit des Datenschutzes (Klarstellung in Art. 8 Abs. 1 Satz 2 E-VDSG)

Die durch den EDÖB vorgeschlagene Prüfung der obenstehenden Garantien durch den Datenexporteur muss sich aufgrund einer positiven Entscheidung des Bundesrats hinsichtlich der Angemessenheit des Datenschutzes in einem Drittstaat erübrigen. Dies folgt bereits daraus, dass ohne die Vorlage solcher Garantien nicht von einem angemessenen Datenschutz ausgegangen werden kann.

Eine zusätzliche Einzelfallprüfung und die damit einhergehende Beurteilung und Entscheidung zur jeweiligen (ausländischen) Rechtsordnung des Importstaates hinsichtlich hinreichender Transparenz und Rechtsschutz für die betroffenen Personen durch den Datenexporteur erscheint darüber hinaus aus Praktikabilitätsgründen weder als durchführbar noch als zielführend.

Denn einerseits sind die relevanten Rechtsgrundlagen, Rechtsprechung sowie insbesondere die Behördenpraxis für (geheime) Zugriffe nicht einheitlich kodifiziert und/oder öffentlich zugänglich. Der Bundesrat und speziell das Eidgenössische Departement für auswärtige Angelegenheiten und das Eidgenössische Justiz- und Polizeidepartement verfügen hier über die besten Quellen und Kenntnisse. Andererseits wäre eine solche Beurteilung als unverhältnismässig aufwändig zu werten, da diese eine Momentaufnahme widerspiegelt, die einem raschen Wandel unterliegen kann. Folglich könnte ein Verantwortlicher gar nicht innert vertretbarer Zeit adäquat auf Änderungen reagieren und sofortige neue Dispositionen treffen.

Darüber hinaus würde der Umstand, Unternehmen als Datenexporteure mit der Aufgabe zu betrauen, die Angemessenheit der Rechtsordnungen des Importstaates zu untersuchen und zu beurteilen, Art. 16 nDSG in Verbindung mit Art. 8 E-VDSG widersprechen. Diese Normen legen fest, dass die Angemessenheitsprüfung und die damit einhergehende Entscheidung vom Bundesrat und nicht von den datenexportierenden Stellen vorgenommen werden muss. Sollte nicht einheitlich der Bundesrat, sondern die datenexportierenden Verantwortlichen solche Beurteilungen vornehmen, sind unterschiedliche Ergebnisse hinsichtlich bestimmter Länder und Datenverarbeitungen vorprogrammiert. Dies würde im Ergebnis trotz viel Aufwand keine Rechtssicherheit schaffen. Die Liste des Bundesrats verlöre dadurch jeden Sinn.

Um eine faktische Aushöhlung der Feststellungskompetenz des Bundesrates sowie unterschiedliche Ergebnisse der Bewertung und eine damit einhergehende Rechtsunsicherheit zu vermeiden, muss deshalb auf Stufe E-VDSG ausdrücklich geklärt werden, dass sich die Verantwortlichen als Datenexporteure auf den Entscheid des Bundesrates zur Angemessenheit verlassen dürfen und keine zusätzlichen Abklärungen treffen müssen.

Daher soll zur Klarstellung ein neuer Satz 2 in Art. 8 Abs. 1 E-VDSG eingefügt werden.

Art. 8 Abs. 1 Satz 2 E-VDSG

[1] Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen~~t werden~~:

a. die internationalen Verpflichtungen des Staates oder internationalen Organs im Bereich des Datenschutzes;
b. die Achtung der Menschenrechte;
c. die geltende Gesetzgebung zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung;
d. die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes;
e. das wirksame Funktionieren von einer oder mehreren unabhängigen Behör-den, die im betreffenden Staat mit dem Datenschutz beauftragt sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen.

Die Verantwortlichen dürfen sich auf den Entscheid des Bundesrates zur Angemessenheit des Datenschutzes nach Satz 1 verlassen und müssen keine zusätzlichen Abklärungen treffen.

2.3 Staaten oder internationale Organe ohne angemessenen Datenschutz (Klarstellung in Art. 8 Abs. 7 E-VDSG [neu])

Alle nicht auf der Liste des Bundesrates aufgeführten Länder gelten per se als Länder mit nicht angemessenem Datenschutz. Wollen Verantwortliche in solche Länder Personendaten versenden bzw. dort bearbeiten (lassen), müssen sie selbst abklären, ob ein angemessener Datenschutz gegeben ist oder andernfalls ergänzend geeignete angemessene Zusatzmassnahmen, z.B. in Form von technischen und organisatorischen Massnahmen treffen. Das Urteil "Schrems II" des EuGH generiert entgegen den Leitlinien des EDÖB vom 18. Juni 2021 in diesem Zusammenhang keine zusätzliche Liste von Ländern mit besonderem Risiko. Dies schon deshalb, weil sachlogisch bei jedem Land mit nicht angemessenem Datenschutz damit zu rechnen ist, dass spezifische Behörden und Stellen wie z.B. Geheimdienste ungefragt Einsicht in die betreffenden Daten nehmen und deshalb auch vom Urteil "Schrems II" erfasst sind. Eine solche Liste von Ländern mit hochgradig nicht angemessenem Datenschutz dürfte auch aus politischen Gründen nicht opportun sein, da sie wichtige internationale Beziehungen der Schweiz nachhaltig gefährden dürfte. Dies ist in Art. 8 E-VDSG im Sinne einer notwendigen Präzisierung klar zu stellen, um obgenannte Leitlinien des EDÖB zu entkräften, sachlogisch in einem neuen Absatz 7.

Sollte an der durch den EDÖB vorgeschlagenen zusätzlichen Prüfung der obenstehenden Garantien, welche aus einer entsprechenden Auslegung der "Schrems II"-Rechtsprechung des EuGH resultiert, festgehalten werden, müsste die Prüfung dieser Garantien sachlogisch ebenfalls einheitlich durch den Bundesrat erfolgen. Dies auch deshalb, weil die Abgrenzung zwischen "nicht angemessen" und "hochgradig nicht

angemessen" sachlogisch zwingend Wertungen beinhaltet, welche gesamthaft einheitlich von einer kompetenten Stelle anzuwenden sind. Nur dadurch wird ein in sich stimmiges Regelungssystem für die gesamte Thematik geschaffen, welches statt Verwirrung tatsächlich Rechtssicherheit schafft. Andernfalls ergäben sich kontraproduktive Widersprüche zwischen der Liste des Bundesrates und den Zusatzlisten der Verantwortlichen. Als Folge davon würde die bereits vorstehend skizzierte Rechtsicherheit (vgl. oben Ziff. 2.2) trotz viel Aufwand sogar noch weiter erhöht.

Eine Einzelfallprüfung und eine damit einhergehende Beurteilung und Entscheidung zur jeweiligen (ausländischen) Rechtsordnung des Importstaates hinsichtlich hinreichender Transparenz und Rechtsschutz für die betroffenen Personen durch den Datenexporteur erscheint aus Praktikabilitätsgründen – wie bereits erwähnt (vgl. oben Ziff. 2.2) – weder als durchführbar noch als zielführend.

Nach alledem ist zur Klarstellung ein neuer Absatz 7 in Art. 8 E-VDSG einzufügen.

Art. 8 Abs. 7 E-VDSG (neu)

[…]

[7] Werden Personendaten ins Ausland in einen Staat oder ein Gebiet ohne angemessenen Datenschutz bekanntgegeben, können ergänzende Massnahmen zu den Garantien gemäss Art. 16 Absatz 2 Buchstabe b und c DSG erforderlich sein, um einen geeigneten Datenschutz zu gewährleisten. Der Bundesrat stellt fest, ob ergänzende Massnahmen erforderlich sind. Die betroffenen Staaten und Gebiete sind im Anhang 1a aufgeführt. Der Entscheid des Bundesrates bezüglich der Erforderlichkeit ergänzender Massnahmen ist verbindlich.

III.2. Art. 9 E-VDSG: Datenschutzklauseln und spezifische Garantien

Die Aufzählung der Anforderungen an ein "Data Transfer Agreement" ist untauglich, weil sie nicht zwischen der Art der Übermittlung bzw. Rollen des Exporteurs und Importeurs unterscheidet. Diese sind jedoch für den Inhalt des Vertrags entscheidend, wie beispielsweise die vom EDÖB inzwischen anerkannten Standardvertragsklauseln der Europäischen Kommission (EU SCC) zeigen.

So macht es keinen Sinn, einen Auftragsbearbeiter im Ausland zur Anwendung der Bearbeitungsgrundsätze, zur Information der betroffenen Personen oder zur Wahrung der Rechte der betroffenen Personen zu verpflichten. Sie müssten dem auch nach dem nDSG nicht nachkommen, weshalb nicht einzusehen ist, dass sie hierzu vertraglich verpflichtet werden sollen.

Zu den einzelnen Buchstaben erlauben wir uns nachfolgende Ausführungen:

- In den Bearbeitungsgrundsätzen (Bst. a) fehlt der Grundsatz der Transparenz.
- Die Anforderungen gemäss Bst. d und e, die Namen der Staaten oder der internationalen Organisationen zu nennen, denen Personendaten bekanntgegeben werden (soweit hiermit Weiterübermittlungen gemeint sind, was nicht klar ist), hat keine rechtliche Grundlage. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Auch die EU SCC beschränken sich darauf.
- Bst. f ist bereits mit dem Grundsatz der Verhältnismässigkeit in Bst. a abgedeckt, damit redundant und zu streichen.

- Aufgrund der in Bst. g sehr allgemeinen Formulierung wird nicht klar, welche Konstellationen hier geregelt werden sollen (z.B. nur die den Vertrag direkt mitunterzeichnenden Empfängerinnen und Empfänger, deren Subakkordanten, weitere vom Vertrag direkt oder indirekt Betroffene, Kunden oder weitere irgendwie Beteiligte?) und welches der konkrete Inhalt der Anforderung sein soll. Um der Anforderung gemäss Bst. g einen klaren und vernünftigen Sinn in Zusammenhang mit der Vertragsgestaltung zu geben, schlagen wir vor, dass hier statt der im Entwurf vorgeschlagenen Formulierung "die Modalitäten für die Weitergabe von Personendaten an Empfängerinnen und Empfänger" aufgeführt werden.
- Für die sehr weit gefasste Anforderung gemäss Bst. j fehlt eine einschlägige gesetzliche Grundlage. Im Gegenteil regelt das nDSG selbst an verschiedenen Stellen bereits umfassend und einlässlich, wer durch wen in welchen Konstellationen zu informieren ist und gegebenenfalls wie (vgl. insb. Art. 16 bis 21 nDSG). Einzelne konkrete Anforderungen, welche darüber hinaus Sinn machen, sind in der E-VDSG bereits ausdrücklich geregelt, namentlich in Art. 13 E-VDSG. Für zusätzliche Anforderungen zwischen den übergeordneten gesetzlichen Anforderungen einerseits und den in Art. 13 E-VDSG geregelten Modalitäten bleibt kein sinnvoller Raum. Die Anforderung von Bst. j ist deshalb als weder zulässig noch sinnvoll ersatzlos zu streichen.
- Es fehlen Regelungen zur Meldung von Verletzungen der Datensicherheit, insbesondere soweit die betroffenen Personen zu informieren sind.

Aus diesen Ausführungen folgt überdies, dass der Anforderungskatalog in Art. 9 Abs. 1 E-VDSG entweder anzupassen ist, um unterschiedliche Konstellationen abzudecken (Verantwortlicher, Auftragsbearbeiter) oder das Wort "mindestens" durch "nach Massgabe der Umstände" zu ersetzen ist. Zudem sind Bst. a um den Grundsatz der Transparenz zu erweitern, die Bst. d, e, f und j zu streichen und Bst. g anzupassen.

In Art. 9 Abs. 2 E-VDSG wird mit "sicherstellen" eine allzu abstrakte Forderung aufgestellt, was der namentlich stark vom Grundsatz der Verhältnismässigkeit geprägten Regelung widerspricht. Entsprechend fordert die Bestimmung richtigerweise auch nur "angemessene" Massnahmen und keinen absoluten Schutz. Um die verschiedenen Teile der Regelung sachlogisch richtig zu verbinden, muss der Begriff "sicherstellen" gestrichen werden.

Demnach ist Art. 9 E-VDSG wie folgt anzupassen:

Art. 9 E-VDSG

[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen ~~mindestens~~nach Massgabe der Umstände die folgenden Punkte regeln:

a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung, ~~und~~ der Richtigkeit und der Transparenz;
b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen;
c. die Art und der Zweck der Bekanntgabe von Personendaten;
~~d. die Namen der Staaten, in die Personendaten bekanntgegeben werden;~~
~~e. die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden;~~
~~f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;~~
g. ~~die zur Bearbeitung der Daten berechtigten~~ die Modalitäten für die Weitergabe von Personendaten an Empfängerinnen und Empfänger;
h. die Massnahmen zur Gewährleistung der Datensicherheit;
i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;
~~j. die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren;~~
k. die Rechte der betroffenen Person, namentlich:
    1. das Auskunftsrecht,
    2. das Widerspruchsrecht,
    3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten,
    4. das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen.

[2] Der Verantwortliche muss angemessene Massnahmen treffen, ~~um sicherzustellen, dass~~ damit die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.

[3] Wurde der EDÖB über die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die:

a. unter denselben Datenschutzklauseln oder Garantien erfolgen, soweit die Kategorien der Empfängerinnen und Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder
b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen Unternehmen, die zum selben Konzern gehören, stattfinden, soweit die Datenschutzklauseln oder Garantien weiterhin einen geeigneten Datenschutz gewährleisten.

III.3. Art. 10 E-VDSG: Standarddatenschutzklauseln

Massnahmen sind angemessen, wenn sie dem Stand der Technik sowie den konkreten Umständen entsprechen. Die Anforderungen an die Massnahmen sind höher, wenn es sich beispielsweise um besonders schützenswerte Personendaten handelt.

Wiederum kann der Exporteur nicht "sicherstellen", sondern nur dafür Sorge tragen (vgl. oben Ziff. III.2).

Der Erläuterungsbericht verlangt fälschlicherweise, dass der Empfänger verpflichtet werden muss, das Schweizer Datenschutzrecht einzuhalten, zumal er ja einer anderen Jurisdiktion untersteht, deren Datenschutzregeln er selbstverständlich einhalten muss. Einhalten muss er insofern nur den Vertrag.

Die Vorschrift führt zu einer Kausalhaftung und ist in der Praxis nicht zu erfüllen. Zudem kennt nicht einmal das Bankenrecht eine derart strenge Regelung.

Aufgrund obiger Ausführungen muss Art. 10 Abs. 1 E-VDSG wie folgt angepasst werden:

Art. 10 E-VDSG

[1] Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so ~~trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.~~trägt er in angemessener Weise Sorge für deren Einhaltung.

[2] Der EDÖB veröffentlicht eine Liste von Standarddatenschutzklauseln, die er genehmigt, ausgestellt oder anerkannt hat.

IV. Pflichten des Verantwortlichen und des Auftragsbearbeiters

IV.1. Art. 13 E-VDSG: Modalitäten der Informationspflichten

1. Streichung des Auftragsbearbeiters und Präzisierung der Vorgaben für eine angemessene Information (Art. 13 Abs. 1 E-VDSG)

In Art. 13 Abs. 1 E-VDSG wird im Verhältnis zum Verantwortlichen – wie auch anderswo (vgl. unten Ziff. IV.2) und entgegen dem Auftragsverhältnis – fälschlicherweise eine identische Verantwortung des Auftragsbearbeiters festgelegt.

Entgegen den Regelungen auf Stufe des nDSG werden die Pflichten des Verantwortlichen gleichzeitig auch dem Auftragsbearbeiter auferlegt. Dies widerspricht der gesetzlichen Regelung. Zudem würde damit auch das zwischen dem Verantwortlichen und seinem Auftragsbearbeiter vertraglich vereinbarte Auftragsverhältnis de facto aufgehoben oder zumindest stark beeinträchtigt und der Verantwortliche verlöre de facto seine Funktion als Geschäftsherr und in diesem Zusammenhang namentlich auch seine Überwachungspflicht gegenüber seinem Auftragsbearbeiter. Die vom Verantwortlichen festgelegten Sicherheitsmassnahmen wären nicht deckungsgleich mit den vom Auftragsdatenbearbeiter in eigener Verantwortung festgelegten dahingehenden Massnahmen. Solche unterschiedlichen Massnahmensets

könnten sich teilweise sogar widersprechen und sich kontraproduktiv auswirken. Die Folge wären unklare Verantwortlichkeiten und übrige Verhältnisse. Mit all dem wäre dem Datenschutz nicht gedient.

Zudem würde die vorgeschlagene Regelung einen unnötigen und kontraproduktiven "Swiss Finish" zur EU-DSGVO produzieren, was den grenzüberschreitenden Verkehr von Personendaten im Verhältnis zur EU erschweren statt erleichtern würde und damit in Widerspruch zu einem der zentralen Gründe für die Revision des Schweizer Datenschutzrechts stünde.

Der Auftragsbearbeiter ist somit als direkt Verantwortlicher sowohl im Titel des 2. Kapitels als auch in Art. 13 Abs. 1 E-VDSG zu streichen.

Zudem sind die Vorgaben für eine angemessene Information zu präzisieren. Mit Blick auf die zunehmend digitale Zukunft ist in diesem Zusammenhang namentlich zu regeln, dass Informationen neu nicht nur auf Papier, sondern auch elektronisch zur Verfügung gestellt werden können. Diese zur Förderung digitaler Geschäftsmodelle sehr wichtige Formel findet sich als Standardformulierung bereits in verschiedenen neueren Gesetzen und Verordnungen, z.B. im FIDLEG (vgl. Art. 9 Abs. 3 FIDLEG), und muss folglich nicht zuletzt auch im Datenschutzrecht realisiert werden.

2. Streichung von Art. 13 Abs. 2 E-VDSG

Es ist nicht klar, was mit "maschinenlesbar" gemeint ist, zumal es sich um einen technisch veralteten Begriff handelt. Ausserdem dürfen Piktogramme ohnehin nur ergänzend verwendet werden. Piktogramme werden zudem unter geltem Recht jedenfalls auf freiwilliger Basis verwendet. Die Verwendung ist grundsätzlich zu fördern. Die freiwillige Verwendung von Datenschutz und Transparenz fördernden Massnahmen sollte nicht mit einschränkenden Anforderungen beeinträchtigt werden. Art. 13 Abs. 2 E-VDSG muss folglich gestrichen werden.

Demzufolge sind der Titel des 2. Kapitels und Art. 13 E-VDSG wie folgt anzupassen:

2. Kapitel: Pflichten des Verantwortlichen ~~und des Auftragsbearbeiters~~

Art. 13 E-VDSG

1 Der Verantwortliche ~~und der Auftragsbearbeiter teilen~~stellt die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form auf Papier oder elektronisch zur Verfügung. ~~mit~~.

~~2 Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~

IV.2. Art. 15 E-VDSG: Information bei der Bekanntgabe von Personendaten

Art. 15 E-VDSG statuiert völlig neue formale zusätzliche Modalitäten und Zusatzpflichten in Zusammenhang mit der Bekanntgabe von Daten an Dritte, welche strikte regelbasiert ohne Differenzierungsmöglichkeit (z.B. entsprechend dem effektiven Risiko) in jedem Fall anwendbar sein sollen. Hierzu findet sich im nDSG keine gesetzliche Grundlage. Im Gegenteil hat das Parlament die Bekanntgabe von Personendaten an Dritte bereits auf Gesetzesstufe an verschiedenen Stellen bereits ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt (vgl. namentlich Art. 16 ff. nDSG). Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen (für Detailbegründung vgl. oben Ziff. I.3 u. A.1-7).

Die Regelung würde inhaltlich zu massiven Zusatzanforderungen buchstäblich bei jeder Art von Kommunikation in Zusammenhang mit Personendaten, z.B. bei jedem einzelnen E-Mail, führen. Damit würden an übliche und vernünftige Kommunikation, selbst solche ohne erkennbare datenschutzrechtliche Risiken, völlig überrissene Anforderungen gestellt. Im operativen Alltag würden damit etablierte, übliche und vernünftige Kommunikationsmittel wie z.B. E-Mail de facto gänzlich verhindert. Solche Ansinnen stehen in vollständigem Widerspruch zu den Anstrengungen des Bundesrats, Digitalisierung und Innovationskraft im Interesse des Wirtschaftsstandorts Schweiz zu fördern.

Dementsprechend finden sich auch im EU-Recht, auf welchen sich der Erläuterungsbericht zu Unrecht beruft, keine solchen Pflichten für private Datenbearbeiter. Art. 15 E-VDSG ist mithin ein für das wesentliche Regulierungsziel der EU-Äquivalenz kontraproduktiver "Swiss Finish".

Somit ist die Regelung am besten gänzlich zu streichen, zumindest aber ausdrücklich auf Bundesorgane einzugrenzen.

Sofern die Regelung nicht gänzlich gestrichen wird, ist zudem auch hier der Auftragsbearbeiter – wie bereits erwähnt – jedenfalls nicht Adressat der Informationspflicht und deshalb zu streichen (vgl. oben Ziff. IV.1).

~~**Art. 15 E-VDSG**~~

~~Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.~~

IV.3. Art. 16 E-VDSG: Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten

Art. 16 E-VDSG entbehrt ebenfalls einer Grundlage im nDSG. Die Pflicht wurde im Rahmen der Vernehmlassung zum nDSG gestrichen und darf umso weniger nicht über die VDSG wieder eingeführt werden. Folglich muss auch diese Bestimmung ersatzlos gestrichen werden (für Details vgl. vorstehend Ziff. IV.2).

~~**Art. 16 E-VDSG**~~

~~Der Verantwortliche informiert die Empfängerinnen und Empfänger, denen er Personendaten bekanntgegeben hat, unverzüglich über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten, ausser die Benachrichtigung ist unmöglich oder mit einem unverhältnismässigen Aufwand verbunden.~~

IV.4. Art. 17 E-VDSG: Überprüfung einer automatisierten Einzelentscheidung

Diese Bestimmung stellt einen Eingriff in die Privatrechtsautonomie dar und kann daher nicht auf Verordnungsstufe verankert werden.

Zudem geht die Regelung von falschen rechtlichen Voraussetzungen aus. Ein allgemeines, generelles Diskriminierungsverbot gibt es nicht. Soweit es direkt aus Grundrechten der Verfassung abgeleitet werden sollte, wäre dies unzulässig, da es keine direkte Drittwirkung verfassungsmässiger Rechte gibt. Eine Diskriminierung wird rechtlich erst dann kritisch, wenn sie rein subjektiv ohne sachlich überzeugende Abgrenzungskriterien erfolgt. All dies ist aber schon deshalb nicht auf Stufe E-VDSG zu regeln, weil das Thema allgemeiner Natur ist und in sämtlichen Rechtsmaterien gleichermassen eine Rolle spielt. Nur schon die etablierte bundesgerichtliche Praxis zum Thema gibt ausreichende Rechtssicherheit.

Eine weitere Präzisierung von Art. 21 nDSG auf Stufe E-VDSG ist weder sinnvoll noch nötig und mangels gesetzlicher Grundlage auch nicht zulässig. Das Parlament hat die Anforderungen an die Informationspflichten bei automatisierten Einzelentscheiden in Art. 21 nDSG bereits ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt. Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen (für Detailbegründung vgl. oben Ziff. I.3 u. A.1-7).

Nach alledem gleichwohl eine solche Regel in die E-VDSG einzuführen, würde unnötigerweise erhebliches Potential für missbräuchliche Klagen gegen Verantwortliche produzieren, welche sich effektiv absolut korrekt und gesetzeskonform verhalten.

Art. 17 E-VDSG ist demnach ersatzlos zu streichen.

~~**Art. 17 E-VDSG**~~

~~Verlangt eine von einer automatisierten Einzelentscheidung betroffene Person, dass sie ihren Standpunkt darlegen kann oder dass eine natürliche Person die Entscheidung überprüft, so darf sie deswegen nicht benachteiligt werden.~~

IV.5. Art. 18 E-VDSG: Form und Aufbewahrung der Datenschutz-Folgenabschätzung

Wie in anderen moderneren Gesetzen auch sollte der Begriff der Schriftlichkeit dahingehend präzisiert werden, dass auch andere Formen erfasst werden, die den Nachweis durch Text ermöglichen. Die von uns vorgeschlagene formelhafte Formulierung entspricht dem derzeit üblichen Gesetzgebungsstandard (vgl. z.B. Art. 5 Abs. 8 FIDLEG).

Die Aufbewahrungspflicht im zweiten Satz von Art. 18 E-VDSG ist mangels gesetzlicher Grundlage im nDSG zu streichen (für Details vgl. oben IV.3). Ausserdem besteht aufgrund des Grundsatzes der Verhältnismässigkeit der Datenbearbeitung sowie der Datenminimierung kein Grund dazu, eine Datenschutz-Folgenabschätzung während zwei Jahren nach Beendigung der Datenbearbeitung aufzubewahren. Schliesslich widersprechen die Ausführungen im Erläuterungsbericht dem Grundsatz "nemo-tenetur", da die Aufbewahrung der Datenschutz-Folgenabschätzungs-Dokumentation gestützt auf ein Editionsersuchen im Vorfeld oder im Rahmen einer rechtlichen Auseinandersetzung zu Beweiszwecken gegen den Verantwortlichen verwendet werden könnte.

Art. 18 E-VDSG müsste daher wie folgt angepasst werden:

Art. 18 E-VDSG

Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in anderer durch Text nachweisbarer Form festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~

IV.6. Art. 19 Abs. 1 und 5 E-VDSG: Meldung von Verletzungen der Datensicherheit

Art. 19 E-VDSG stellt eine Präzisierung von Art. 24 nDSG dar und ist so zu verstehen, dass im Falle einer Meldung an den EDÖB diese die in Art. 19 Abs. 1 VDSG aufgeführten Punkte enthalten muss.

Die Einschränkung "soweit möglich" macht Sinn, da die Angabe in der Praxis oft nicht möglich ist.

Bst. a und b gehen über die DSGVO hinaus, doch dürfte dies in der Praxis kein Problem darstellen.

Falsch formuliert ist hingegen Bst. e. Die "allfälligen Risiken" beinhalten bereits die Folgen für die betroffenen Personen. Richtig müsste es heissen "die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht".

Auch in Bst. f muss nicht von den "Folgen", sondern vom "Risiko " die Rede sein. Gemildert werden kann entweder das Schadensausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem "Risiko" entspricht). Bei Bst. f ist zudem zu präzisieren, dass es nur um Massnahmen gehen kann, welche der Verantwortliche tatsächlich ergriffen hat ("gegebenenfalls").

Gemäss den Erläuterungen wird das in Art. 24 Abs. 1 nDSG erwähnte "voraussichtlich" so interpretiert, dass auch dann gemeldet werden muss, wenn das Vorliegen eines "hohen Risikos" nicht ausgeschlossen werden kann. Diese Aussage hilft nicht weiter, da es sich um einen Pleonasmus handelt. Der Begriff "Risiko" beinhaltet bereits eine Wahrscheinlichkeitsüberlegung, d.h. wie wahrscheinlich es ist, dass ein Schaden eintritt. Es bleibt dabei: Die Wahrscheinlichkeit muss eine gewisse Höhe aufweisen.

Wünschenswert wäre zusätzlich eine "de minimis"-Regelung, die jene Fälle ausschliesst, in welchen der EDÖB ohnehin nicht wirklich etwas tun kann oder will (z.B. eine problematische E-Mail geht an den falschen Empfänger und ein Missbrauch durch diesen ist möglich). Damit können auch die Ressourcen des EDÖB geschont werden, die er für andere, für den Datenschutz wichtigere Angelegenheiten einsetzen kann.

Schliesslich entbehrt die Dokumentationspflicht gemäss Art. 19 Abs. 5 E-VDSG einer gesetzlichen Grundlage. Eine solche Regelung ist auch weder sinnvoll noch nötig. Das Parlament hat die Anforderungen an die Pflicht zur Meldung von Verletzungen der Datensicherheit bereits auf Gesetzesstufe ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt (vgl. Art. 24 nDSG). Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen (für Detailbegründung vgl. oben Ziff. I.3 u. A.1-7). Daran kann der Umstand, dass die EU-DSGVO eine ausdrückliche Dokumentationspflicht kennt, nichts ändern. Der klare Entscheid des Parlaments verbietet jedenfalls, auf Verordnungsstufe gleichwohl eine Dokumentationspflicht einführen zu wollen.

Folglich ist Absatz 5 ersatzlos zu streichen.

Art. 19 E-VDSG

[1] Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit:

a. die Art der Verletzung
b. soweit möglich den Zeitpunkt und die Dauer;
c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;
d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;
e. die Folgen~~, einschliesslich der allfälligen Risiken,~~ für die betroffenen Personen, von welchen ein hohes Risiko ausgeht;
f. gegebenenfalls welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder ~~die Folgen~~ das Risiko zu mildern;
g. den Namen und die Kontaktdaten einer Ansprechperson.

[2] Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

[3] Der Verantwortliche teilt den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mit.

[4] Handelt es sich beim Verantwortlichen um ein Bundesorgan, so erfolgt die Mel-dung an den EDÖB über die Datenschutzberaterin oder den Datenschutzberater.

~~[5] Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.~~

V. Auskunftsrecht

V.1. Art. 20 Abs. 3 und 5 E-VDSG: Modalitäten

Art. 20 Abs. 3 E-VDSG verlangt, dass die Auskunft verständlich sein muss. Dies bedeutet nicht, dass der Verantwortliche der um Auskunft ersuchenden Person die Datensätze oder darüber hinausgehend sogar die damit einhergehenden Abläufe und Geschäftsmodelle erklären muss. Dies könnte im Einzelfall je nach Person mit enormem und unverhältnismässigem Aufwand verbunden sein und wäre je nach Person u.U. gleichwohl untauglich. Zudem könnte eine solche Regelung auch dazu missbraucht werden, das Verfahren und damit den Aufwand für den Verantwortlichen ohne sachlichen Grund "künstlich" zu verlängern.

Vielmehr muss ausreichend sein, die herauszugebenden Daten so aufzubereiten und darzustellen, dass sie geordnet sind und dadurch unter Anwendung eines objektivierten Masstabes nach Treu und Glauben verständlich sind oder sein müssen. Ob die betroffene Person diese Darstellung im konkreten Fall tatsächlich versteht, kann nicht relevant sein, geht es doch beim datenschutzrechtlichen Auskunftsbegehren nur darum, die bearbeiteten Daten mitzuteilen. Dies entspricht dem Kern des Auskunftsanspruchs, welcher

die effektive Herausgabe der relevanten Daten sicherstellt. Darüber hinaus besteht keine Pflicht des Verantwortlichen, die Daten, deren Zweck oder – damit zusammenhängend – die Art der Datenhaltung oder sogar die Geschäftsabläufe zu erläutern. Solches ist schon deshalb abzulehnen, weil dadurch der Aufwand unermesslich und im Einzelfall sogar "never ending" werden könnte. Beispielsweise können die im Rahmen einer klinischen Studie bearbeiteten Daten oder technische Logdaten für die betroffene Person unverständlich sein. Müssen diese zuerst so dargestellt werden, dass sie für die betroffene Person verständlich sind, kann dies oft nicht innerhalb von 30 Tagen erfolgen. Damit würde der Grundsatz der Auskunftserteilung innert 30 Tagen entgegen der gesetzlichen Absicht regelmässig zur Ausnahme.

Will die auskunftsberechtigte Person mehr über solche über den eigentlichen Herausgabeanspruch hinaus gehende Verhältnisse erfahren, muss sie sich an einen Rechtsanwalt oder Wirtschaftsfachmann halten, nicht an den Verantwortlichen. Demzufolge ist Absatz 3 zusätzlich dahingehend zu klären, dass über die eigentliche "geordnete" Datenherausgabe "keine zusätzlichen Erläuterungen erforderlich" sind.

Da die Aktivität und die damit einhergehende Verständlichkeit der Auskunft vom Verantwortlichen ausgeht und von diesem gesteuert werden kann und muss, macht es Sinn, den Verantwortlichen hier bei Absatz 3 mit Bezug auf die Formulierung in den Aktiv-Modus zu setzen.

Die Dokumentationspflicht und namentlich die Aufbewahrungsfrist von mindestens 3 Jahren gemäss Art. 20 Abs. 5 E-VDSG entbehren einer ausreichenden gesetzlichen Grundlage. Das Parlament hat die Anforderungen an das Auskunftsbegehren auf Gesetzesstufe ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt (vgl. Art. 25 bis 27 nDSG). Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen (für Detailbegründung vgl. oben Ziff. I.3 u. A.1-7).

Absatz 5 ist deshalb ersatzlos zu streichen.

Nach alldem ist Art. 20 E-VDSG wie folgt anzupassen:

Art. 20 E-VDSG

[1] Das Auskunftsbegehren wird schriftlich gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden.

[2] Die Auskunft wird in der Regel schriftlich erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat.

[3] Der Verantwortliche muss d~~D~~ie Auskunft ~~muss für die betroffene Person verständlich sein~~geordnet vornehmen. Zusätzliche Erläuterungen sind nicht erforderlich.

[4] Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.

~~[5] Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.~~

V.2. Art. 21 E-VDSG: Zuständigkeiten und Abgrenzungen

Der zweite Satz von Art. 21 Abs. 1 E-VDSG stellt eine Forderung auf, welche im operativen Alltag regelmässig gar nicht erfüllt werden kann.

In manchen Konstellationen ist für einen Verantwortlichen weder klar noch eindeutig ersichtlich, inwieweit für einen bestimmten Sachverhalt ein anderer Verantwortlicher zuständig sein soll und wer dies gegebenenfalls ist. In vielen Fällen kann ein Verantwortlicher deshalb der Pflicht, das Begehren an den zuständigen Verantwortlichen weiterzuleiten, naturgemäss gar nicht nachkommen. In unklaren Fällen ein Auskunftsbegehren an andere, vermeintlich zuständige Verantwortliche weiterzuleiten, würde dem Datenschutz geradezu entgegenlaufen, erhielten doch auf diese Weise womöglich Personen Kenntnis vom Fall, welche gar nicht als Verantwortliche qualifizieren. Einer fälschlicherweise um Auskunft ersuchten Person ist es auch nicht zuzumuten, abzuklären, wer an seiner Stelle Verantwortlicher sein könnte. Auch solche Abklärungen würden dem berechtigten Bedürfnis der um Auskunft ersuchenden Person um Einhaltung des Datenschutzes gerade zuwiderlaufen.

Der erste Satz von Art. 21 Abs. 1 E-VDSG ist deshalb dahingehend zu präzisieren, dass es nur um Daten gehen kann, für welche mehrere Verantwortliche "gemeinsam" verantwortlich sind. Auch bei solchen Konstellationen ist zu berücksichtigen, dass es beim Auskunftsbegehren um besonders schützenswerte Daten gehen kann, welche sich aus der Begründung der anspruchsberechtigten Person ergeben können. Zudem können trotz gemeinsamer Verantwortung auf Detailstufe unterschiedliche Datensätze je Verantwortlichen vorliegen. Ein Auskunftsbegehren darf deshalb nicht ohne Weiteres in die Disposition eines Verantwortlichen zur Weiterleitung an weitere Personen gestellt werden. Abgesehen davon können sich besondere Herausforderungen betreffend Erreichbarkeit von anderen, eventuell im fernen Ausland

domizilierten Verantwortlichen und damit grössere zeitliche Verzögerungen ergeben. Dies namentlich auch deshalb, weil Auskunftsbegehren aus naheliegenden Gründen nicht mit ungesichertem E-Mail weitergleitet werden dürfen. Ungesicherte E-Mails werden digital nicht als verschlossener Brief, sondern quasi als Postkarte wahrgenommen und können somit potenziell von unbekannten Dritten ungehindert eingesehen werden. Solche Weiterleitungen wären somit per se eine potenzielle Verletzung datenrechtlicher Pflichten. Aus diesen Gründen ist der erste Satz von Absatz 1 offener zu formulieren, indem lediglich die Pflicht zur Koordination statuiert wird. Umgekehrt ist der zweite Satz von Absatz 1 ersatzlos zu streichen.

Zudem regeln die Absätze 1 und 2 identische Themen. Es geht um den koordinierten Umgang mit einem Auskunftsbegehren bei mehreren Verantwortlichen. Ob sich unter diesen "mehreren Personen" auch noch ein Auftragsdatenbearbeiter befindet, spielt mit Bezug auf in der hier zu regelnden Notwendigkeit der Koordination keine Rolle. Wird der Absatz 1 entsprechend vorstehender Begründung angepasst, kann demzufolge Absatz 2 ersatzlos gestrichen werden.

Gleichzeitig regen wir an, diese Verhältnisse im abschliessenden **Erläuterungsbericht** prägnant darzustellen. Dies führt zu folgender Neufassung von Art. 21 E-VDSG:

Art. 21 E-VDSG

1 Sind für die Bearbeitung von Personendaten mehrere gemeinsam verantwortlich, so ~~kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen~~ sollen sie sich nach Möglichkeit koordinieren. ~~Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.~~

~~2 Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern er nicht in der Lage ist, das Begehren selbst zu beantworten.~~

Sollten Sie diesem Antrag wider Erwarten nicht folgen, wäre zusätzlich zu berücksichtigen, dass Absatz 2 von Art. 21 E-VDSG verwirrlich formuliert und deshalb auf jeden Fall korrigiert werden müsste. In der aktuellen Fassung impliziert Absatz 2, dass der Auftragsdatenbearbeiter selbst eine Auskunftspflicht hat, wenn er faktisch in der Lage sein sollte, eine Auskunft zu erteilen bzw. dass er das Auskunftsgesuch in einem solchen Fall nicht weiterleiten muss, auch wenn er es nicht beantwortet. Das kann nicht sein. Der letzte Halbsatz von Absatz 2 ("sofern er nicht in der Lage ist, das Begehren selbst zu beantworten") wäre zu streichen und durch die Formulierung "sofern dieser das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet" zu ersetzen.

Im Eventualfall müsste Art. 21 E-VDSG somit wie folgt angepasst werden:

Art. 21 E-VDSG

[1] Sind für die Bearbeitung von Personendaten mehrere gemeinsam verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. ~~Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.~~

[2] Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern dieser das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet ~~in der Lage ist, selbst Auskunft zu erteilen~~.

V.3. Art. 22 Abs. 1 E-VDSG: Frist

Der Fristbeginn muss in Art. 22 Abs. 1 E-VDSG präzisiert werden. Sollte ein Auskunftsbegehren nicht klar sein und eine Präzisierung erfordern, soll entsprechend die 30-tägige Frist erst mit Zugang der Präzisierung zu laufen beginnen. Auch Unklarheiten über die Identifikation der um Auskunft ersuchenden Person können solche Unklarheiten produzieren. Dies ist namentlich bei Banken der Fall, wo ergänzend zu datenschutzrechtlichen Regeln auch diejenigen des Bankkundengeheimnisses (Art. 47 BankG) zu beachten sind. Auch diesfalls darf die Frist entsprechend erst nach Klärung des Sachverhalts zu laufen beginnen.

Art. 22 Abs. 1 E-VDSG ist demnach wie folgt zu ergänzen:

Art. 22 Abs. 1 E-VDSG

[1] Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Erfordert das Begehren einer Präzisierung, welche Daten die betroffene Person wünscht, beginnt die Frist mit Zugang der Präzisierung und gegebenenfalls der Identifikation beim Verantwortlichen zu laufen. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen.

[2] Kann die Auskunft nicht innert 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber benachrichtigen und ihr die Frist mitteilen, in der die Auskunft erfolgen wird.

V.4. Art. 23 E-VDSG: Ausnahmen von der Kostenlosigkeit

Der Maximalbetrag von CHF 300.- wird den tatsächlichen Verhältnissen und dem damit verbundenen Aufwand nicht ansatzweise gerecht. Sind z.B. zur Sicherstellung des Datenschutzes von Dritten umfangreiche Schwärzungen notwendig, kann dies im Einzelfall Aufwendungen von durchaus CHF 10'000.- mit sich bringen. Art. 23 Abs. 2 E-VDSG sollte deshalb gestrichen werden, da die angemessene Kostenbeteiligung bereits in Absatz 1 enthalten ist. Um besonders aufwendigen Fällen vorgenannter Art

gerecht zu werden, könnte als Variante in Absatz 2 auch geregelt werden, dass die ersten CHF 500.- des anfallenden Aufwandes vom Verantwortlichen allein und die Zusatzkosten je hälftig zu übernehmen sind.

Des Weiteren muss in Absatz 3 verhindert werden, dass die von Art. 23 Abs. 1 E-VDSG zur Verfügung gestellte Frist von 30 Tagen zur Auskunftserteilung faktisch auf 20 Tage abgekürzt wird, weshalb der Fristbeginn in Art. 23 Abs. 3 E-VDSG präzisierend ergänzt werden muss.

Art. 23 E-VDSG

[1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden, oder querulatorisch ist.

~~[2] Die Beteiligung beträgt maximal 300 Franken.~~

[3] Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen. Die Frist zur Auskunftserteilung beginnt mit Ablauf der Rückzugsfrist.

VI. Besondere Bestimmungen zur Datenbearbeitung durch private Personen

VI.1. Datenschutzberaterin oder -berater

1. Art. 25 Abs. 1 Bst. a und b E-VDSG

Die Datenschutzberaterin oder der Datenschutzberater muss lediglich beratend Einfluss nehmen, damit der Verantwortliche die Datenschutzpflichten richtig anwendet (vgl. Art. 10 nDSG, insb. Abs. 2 Bst. b).

Bei der Formulierung von Art. 25 Abs. 1 Bst. a E-VDSG bleibt mit der lapidaren Formulierung "prüft" der Umfang der Prüfpflicht unklar. Die Funktion Datenschutzberatung kann jedenfalls nicht jede beim Verantwortlichen anfallende Datenbearbeitung prüfen. Dies wäre nicht nur mit Blick auf die schiere Anzahl von anfallenden Bearbeitungen objektiv unmöglich, sondern auch, weil die Funktion Datenschutzberatung auch gar nicht jede prüfenswerte Datenbearbeitung effektiv kennen kann. Der Verantwortliche kann aber in Absprache mit der Funktion Datenschutzberatung eine interne Governance schaffen, welche in geeigneter Form die internen Regeln zu diesem Thema festlegt, z.B. mit Weisungen und Prozessen, welche entsprechend auch Aufgaben, Kompetenzen und Verantwortlichkeiten festlegen. Dabei muss keineswegs immer die Funktion Datenschutzberatung als verantwortlich bezeichnet werden. Für diese ist nach dem Gesagten mit Bezug auf Prüfungen sinnvollerweise eine Konsultationspflicht festzulegen. M.a.W. muss die Funktion Datenschutzberatung nur solche Datenbearbeitungen prüfen, welche ihr effektiv vorgelegt werden. Dies auch zum eigenen Schutz. Die interne Governance sollte eine solche Konsultationspflicht sinnvollerweise noch weiter spezifizieren, z.B. auf bestimmte besonders komplexe Themen wie z.B. Outsourcing oder Konstellationen mit besonders weitreichenden Folgen und damit einhergehenden potenziellen Risiken eingrenzen. Ausserhalb der Konsultationspflicht muss die Funktion Datenschutzberatung entsprechend ihrer Hauptfunktion nur allgemein beratend tätig sein. Zur Klarstellung dieser Verhältnisse ist – auch zum Schutz von Datenschutzberatern, für welche keine spezifische interne Governance besteht - die in Art. 25 Abs. 1 Bst. a genannte Prüfpflicht auf "ihm vorgelegte"

Datenbearbeitungen einzugrenzen. Weitere Erläuterungen im vorstehenden Sinn sollten zusätzlich im abschliessenden **Erläuterungsbericht** dargestellt werden.

Die Regelung von Art. 25 Abs. 1 Bst. b E-VDSG widerspricht der Funktion Datenschutzberatung und überdies der Organisationsfreiheit des Verantwortlichen, wie genau die Pflichten gemäss nDSG unter Würdigung der konkreten Verhältnisse im Unternehmen personell, technisch und organisatorisch am besten erfüllt werden sollen. Insofern liegt ein nicht stufengerechter Eingriff in die Privatautonomie des Unternehmens als Verantwortlichem vor.

Sie widerspricht der vorstehend erläuterten Beratungsfunktion und setzt sich überdies in Widerspruch zu zahlreichen branchenspezifischen Regelungen, im Bereich von Finanzdienstleistern, z.B. mit dem FINMA-Rundschreiben 2017/1 Corporate Governance - Banken und sowie dem FINMA-Rundschreiben 2017/2 Corporate Governance - Versicherer. Demgemäss stellt die Regelung auch eine Verletzung aufsichtsrechtlicher Vorgaben zahlreicher regulierter Branchen mit hohem Grad an Arbeitsteilung dar. Datenschutz ist eine typische Querschnittsmaterie mit einer sehr hohen Arbeitsteilung, unter Einbezug zahlreicher Experten aus unterschiedlichen Bereichen. Die Datenschutzberaterin oder der Datenschutzberater kann nicht von einer einzigen Person bzw. Funktion wahrgenommen werden. Die Funktion der Datenschutzberatung kann höchstens eine formelle Prüfung vornehmen, d.h. im Rahmen einer Selbstdeklaration Auskünfte von für bestimmte Datenbearbeitungen verantwortlichen Stellen einholen. Die tatsächliche Überprüfung der Funktionsweise und Qualität einer Datenbearbeitung wird eine Datenschutzberaterin oder ein Datenschutzberater typischerweise nicht selbst durchführen können. Dies liegt in der Verantwortung der jeweiligen Verantwortlichen. Alles andere wäre ein krasses Übernahmeverschulden, das zahlreiche auch arbeits- und vertragsrechtliche Sorgfaltspflichtverletzungen nach sich ziehen würde.

Ferner verletzt die Bestimmung das weltweit als Standard etablierte Drei-Linien-Verteidigungsmodell, in dem es die Erkennung, Einhaltung und Korrektur von datenschutzrechtlichen Vorgaben einer einzelnen Funktion, namentlich der Datenschutzberaterin oder dem Datenschutzberater, auferlegt.

Schliesslich macht die vorgeschlagene Regelung von Art. 25 Abs. 1 Bst. b E-VDSG die übergeordnete Ausnahmeregelung von Art. 23 Abs. 4 nDSG obsolet oder anders gesagt: Art. 25 Abs. 1 Bst. b E-VDSG ist gar nicht nötig, weil mit Art. 23 Abs. 4 nDSG bereits eine ausreichende übergeordnete Regelung besteht.

Nach alledem ist Art. 25 Abs. 1 Bst. b E-VDSG ersatzlos zu streichen. Dementsprechend kann Art. 25 Abs. 1 Bst. a E-VDSG direkt in Abs. 1 integriert werden, was die Regelung etwas kürzer macht.

Demgemäss sollte Art. 25 Abs. 1 E-VDSG ohne ausdrückliche Bst. a wie folgt neu formuliert werden:

Art. 25 Abs. 1 E-VDSG

[1] Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen ~~muss folgende Aufgaben wahrnehmen:~~

~~a. Sie oder er~~ prüft die ihm vorgelegten Bearbeitungen von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass rechtliche Datenschutzvorschriften verletzt wurden.

~~b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.~~

2. Art. 25 Abs. 2 Bst. c E-VDSG (neu)

Das Interventionsrecht gemäss Bst. b ist zur Vervollständigung einer konzeptionell in sich stimmigen "Good Governance" mit dem Eskalationsrecht in einer neuen Bst. c zu ergänzen.

Art. 25 Abs. 2 Bst. b E-VDSG regelt zu Recht ein Interventionsrecht. Dies ist nötig, damit die Datenschutzberaterin oder der Datenschutzberater bei unternehmensinternen Prüfungen der Einhaltung datenschutzrechtlicher Regeln nicht nur den Worten bzw. den ihr oder ihm zur Verfügung gestellten Dokumenten vertrauen muss, sondern – soweit sinnvoll und nötig – die Beschaffung zusätzlicher Informationen und Dokumente durchsetzen kann. Mit dieser Regelung bleibt Art. 25 Abs. 2 Bst. b E-VDSG aber "auf halbem Weg" stehen. Stösst die Datenschutzberaterin oder der Datenschutzberater nämlich bei der Ausübung des Interventionsrechts auf Unstimmigkeiten und sind die Linienverantwortlichen nicht gewillt, entsprechend dem Ratschlag der Datenschutzberaterin oder des Datenschutzberaters Abhilfe zu schaffen, muss Letztere oder Letzterem spiegelbildlich zum Interventionsrecht bzw. zur Vervollständigung des Gesamtprozesses überdies ein Eskalationsrecht zustehen. Ein solches Recht ist sachlogisch keine Pflicht. Die Datenschutzberaterin oder der Datenschutzberater erhält damit aber das notwendige Instrumentarium, zumindest im Fall komplexer Verhältnisse und besonders schwerwiegende Verstösse gegen Datenschutzpflichten notfalls, mithin als Ausnahme von der Regel, die Thematik im Rahmen und allenfalls in Absprache mit der Compliance-Organisation, soweit eine solche besteht, auf dem Linienweg nach oben zu eskalieren und auf diese Weise auf höherer Stufe zum Entscheid zu bringen bzw. bringen zu lassen, nötigenfalls bis zum höchsten Organ des Unternehmens, und damit klare Verhältnisse zu schaffen. Bei einfacheren Strukturen genügt es aber auch, wenn die Funktion Datenschutzberatung in wichtigen Fällen die höchsten Organe lediglich informiert. Andernfalls setzt sich die Datenschutzberaterin oder der Datenschutzberater gerade bei schwerwiegenden Verstössen gegen Datenschutzpflichten dem Risiko aus, mangels Eskalationsmöglichkeit im Schadensfall selbst haftbar zu werden, weil ihr oder ihm vorgeworfen wird, sich nicht hartnäckig genug eingesetzt zu haben. Art. 25 Abs. 2 ist somit mit einer Bst. c zu ergänzen, welche ergänzend zum Interventionsrecht nach Bst. b das Eskalationsrecht regelt.

Deshalb ist Art. 25 Abs. 2 E-VDSG um eine neuen Bst. c wie folgt zu ergänzen:

Art. 25 Abs. 2 Bst. c E-VDSG (neu)

[2] Der private Verantwortliche muss der Datenschutzberaterin oder dem Datenschutzberater:

a. die notwendigen Ressourcen zur Verfügung stellen;
b. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.
c. das Recht einräumen, in wichtigen Fällen, die höchsten Organe zu informieren.

VI.2. Art. 26 E-VDSG Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

1. Anzahl Mitarbeitende

Vorab ist mit Blick auf die wichtigen Regulierungsziele des Schutzes von Daten natürlicher Personen sowie der Entlastung von KMU davon auszugehen, dass mit dem zahlenmässigen Abgrenzungskriterium "250" effektiv angestellte Mitarbeitende gemeint sind, unabhängig von ihrem Beschäftigungsgrad. Der Beschäftigungsgrad wäre auch ein wenig präzises Kriterium, da dieser in der heutigen Zeit zunehmender Arbeitsteilung und je nach Wirtschaftslage laufenden Schwankungen unterworfen ist.

Zudem ist die Bedeutung der Aufgreifkriterien in Bst. a und b unklar. Richtigerweise müssen Unternehmen mit 250 oder mehr Mitarbeitenden sachlogisch nur diejenigen Bearbeitungstätigkeiten in Verzeichnissen dokumentieren, welche die in Bst. a und b genannten Kriterien erfüllen, d.h. eine Datenbearbeitung durchführen, die ein hohes Risiko mitbringt.

Vorstehende Präzisierungen zur Berechnungsweise der Anzahl Mitarbeitenden müssen zur Schaffung von Rechtssicherheit im abschliessenden **Erläuterungsbericht** dargestellt werden.

2. Verzeichnis der Bearbeitungstätigkeiten

Sind die Voraussetzungen für die Befreiung nicht erfüllt, ist das Verzeichnis für alle Bearbeitungsaktivitäten zu führen. Dies impliziert jedenfalls der Wortlaut von Art. 26 E-VDSG. Die EU-DSGVO ist in diesem Punkt strenger. Art. 12 Abs. 5 nDSG erlaubt die Ausnahme nur, wenn ein "geringes Risiko" vorliegt. Demnach geht der Bundesrat davon aus, dass bei Nichterfüllung der Sachverhalte von Art. 26 Bst a und b E-VDSG per se ein geringes Risiko vorliegt. Dies schränkt allerdings den Anwendungsbereich der Datenschutz-Folgenabschätzung gemäss Art. 22 nDSG ein.

Zudem sind diese Ausnahmen in den Art. 3 und 4 E-VDSG nicht vorgesehen, was zu absurden Folgen führen kann. Soweit unserem Antrag, ebendiese Art. 3 und 4 der E-VDSG zu streichen, richtigerweise stattgegeben wird, wird auch dieser Widerspruch behoben. Andernfalls wäre er selbstverständlich aufzuheben, und zwar dadurch, dass diese Ausnahmen zwecks Sicherstellung einer in sich stimmigen Rechtsordnung auch bei Art. 3 und 4 zugestanden werden.

3. Notwendigkeit einer Übergangsfrist

Solche Verzeichnisse können naturgemäss erst gestützt auf das Vorliegen eines umfassenden, in sich stimmigen Gesamtkonzepts sämtlicher Regeln bzw. Pflichten zielführend und final festgelegt werden. Deshalb sollte dafür auf Verordnungsstufe eine generelle Übergangsfrist festgelegt werden (vgl. unten Ziff. VII.), welche sachlogisch auch die Anwendbarkeit der Regelung von Art. 26 E-VDSG miterfasst.

VII. Übergangsbestimmungen

Die Übergangsfristen im nDSG sind punktuell und lückenhaft (vgl. Art. 69 bis 72 nDSG). Dieses lückenhafte Übergangsregime auf Stufe des nDSG ist auf Verordnungsstufe mit zusätzlichen Übergangsbestimmungen zu ergänzen.

Für sämtliche neuen Pflichten, welche erheblichen Aufwand generieren, müssen angemessene Übergangfristen bestehen, zumal IT-gestützte Lösungen nötig sind.

Dabei ist zu berücksichtigen, dass die verschiedenen Regeln und Pflichten des gesamten Regelwerks (Gesetz samt Verordnung) gegenseitige Wechselwirkungen generieren. Die neuen Regeln bzw. Pflichten sind deshalb zusammen mit den unverändert weiter geltenden Regeln bzw. Pflichten zu einem in sich stimmigen Gesamtkonzept zu verschmelzen. Ein solches Gesamtkonzept kann sachlogisch erst nach Vorliegen der finalen Texte auf Gesetzes- und Verordnungsstufe erarbeitet, final festgelegt und umfassend in die IT-Sprache "übersetzt" werden. Erst danach kann mit dem Aufbau der IT-gestützten Lösung begonnen werden. Vor der "Go live"-Schaltung sind sodann die nach bewährten Standards vorgesehenen Tests durchzuführen. Parallel dazu sind auch die Mitarbeitenden entsprechend ihrer jeweiligen Funktion auszubilden und überdies die Verträge mit Lieferanten und Geschäftspartnern anzupassen.

Für alle diese notwendigen Aktivitäten ist gemäss etablierten Erfahrungswerten ein Zeitraum von rund 2 Jahren ab Vorliegen der finalen Gesetzes- und Verordnungstexte notwendig. Im Gegenzug stellt eine solche IT-gestützte Lösung die gleichförmige Anwendung sämtlicher Regeln innerhalb des gesamten Unternehmens sicher.

Aus den genannten Gründen hat die EU seinerzeit entschieden, für die Umsetzung der EU-DSGVO nicht Übergangsfristen für einzelne Regeln bzw. Pflichten, sondern pauschal 2 Jahre für das gesamte Regelwerk zuzugestehen.

In der Schweiz hat das Parlament für das nDSG eine andere Grundentscheidung getroffen (vgl. Art. 68 bis 74 nDSG). Im Rahmen des parlamentarischen Prozesses liegt der Fokus naturgemäss auf den materiellen Regeln bzw. Pflichten. Das kam beim nDSG besonders deutlich zum Ausdruck, wurde doch über den konkreten Wortlaut einiger zentraler Bestimmungen wie z.B. zum Profiling (Art. 5 Bst. f und g nDSG) buchstäblich bis zum Schluss heftig debattiert. Die Übergangsbestimmungen kommen deshalb im parlamentarischen Prozess regelmässig zu kurz, was beim nDSG in erhöhtem Mass der Fall war. Übergangsbestimmungen sollen zudem strikte nach sachlichen Kriterien festgelegt werden und nicht "Spielball" politischer Kompromisse sein. Deshalb hat es sich im schweizerischen Gesetzgebungsprozess inzwischen eingebürgert, falls notwendig ergänzende Übergansbestimmungen auf Verordnungsstufe festzulegen.

Im Zuge der DSG-Revision ist zumindest für folgende entweder neu eingeführten oder zumindest mit neuen Anforderungen konfrontierten Regeln bzw. Pflichten mit offensichtlich erheblichem Umsetzungsbedarf auf Gesetzesstufe keine Übergangsbestimmung festgelegt worden:

- Pflicht, eine angemessene Datensicherheit zu gewährleisten (Art. 8 nDSG i.V.m. Art. 1 ff. E-VDSG);
- Pflicht zur Erstellung des Verzeichnisses der Datenbearbeitungstätigkeiten (Art. 12 nDSG);
- Pflicht, so rasch als möglich Meldung von Verletzungen der Datensicherheit zu erstatten (Art. 24 nDSG i.V.m. Art. 19 E-VDSG).

Gerade diese drei zentralen Pflichten können naturgemäss erst gestützt auf das Vorliegen eines umfassenden, in sich stimmigen Gesamtkonzepts sämtlicher Regeln bzw. Pflichten zielführend und final festgelegt werden. Dies trifft in besonderem Masse auf die Datensicherheit zu. Zwar bestehen solche Anforderungen selbstredend schon heute. Allerdings muss die Datensicherheit auch das entsprechend nDSG gegenüber vorher völlig veränderte Datenschutzkonzept und das damit eng zusammenhängende und sachlogisch ebenfalls völlig veränderte Datenmanagement abdecken.

Der finale Wortlaut der E-VDSG wird wohl erst gegen Ende des Jahres 2021 vorliegen. Unter Mitberücksichtigung des Umstandes, dass gestützt auf den Wortlaut des nDSG mit den Umsetzungsarbeiten zumindest schon begonnen werden konnte, ist nach dem Gesagten für die drei vorgenannten Pflichten eine Übergangsfrist bis allermindestens 1. Juli 2023 notwendig.

> **Art. 48 ~~Inkrafttreten~~Übergangsbestimmung betreffend die formellen Anforderungen an die Datensicherheit, das Verzeichnis der Bearbeitungstätigkeiten und der Meldung von Verletzungen der Datensicherheit**
> ~~Diese Verordnung tritt am ... in Kraft.~~ Art. 12 und 24 des Gesetzes sind erst ab 1. Juli 2023 zu erfüllen.

In der Folge würde Art. 48 E-VDSG (Inkrafttreten) neu zu Art. 49 E-VDSG.

> **Art. ~~48~~49 Inkrafttreten**
> Diese Verordnung tritt am ... in Kraft.

Alternativ zum neuen Art. 48 E-VDSG kann stattdessen das Inkrafttreten des ganzen Gesetzgebungspakets (nDSG und E-VDSG) nach hinten auf den 1. Juli 2023 geschoben werden, da zwischen Inkrafttreten und Übergangsfristen ein "dynamisches Gleichgewicht" besteht.

Wir bitten Sie schliesslich höflich, die jeweiligen Bestimmungen des nDSG – analog beispielsweise zur BankV oder zur FIDLEV – in den Bestimmungen der vorliegenden VDSG aufzunehmen.

Swiss Banking

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme und die Berücksichtigung unserer Überlegungen für die weiteren Arbeiten. Gerne stehen wir Ihnen für ergänzende Auskünfte zur Verfügung, selbstverständlich auch im Rahmen einer Sitzung.

Freundliche Grüsse
Schweizerische Bankiervereinigung

Andreas Barfuss
Leiter Legal & Compliance

Natalie Graf
Fachverantwortliche Legal

Per Email
fanny.matthey@bj.admin.ch
daniela.nueesch@bj.admin.ch

Zürich, 24. September 2021

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Matthey
Sehr geehrte Frau Nüesch
Sehr geehrte Damen und Herren

Der Schweizerische Leasingverband (SLV) vertritt die Interessen der Schweizer Leasinggesellschaften. Gerne äussern wir uns im Rahmen der oben genannten Vernehmlassung wie folgt zum Verordnungsentwurf bzw. zu den einzelnen Verordnungsbestimmungen:

Am 25. September 2020 hat das Parlament – nach langen Debatten – die Totalrevision des Schweizer Datenschutzgesetzes (revDSG) verabschiedet. Dieses ist international abgestimmt, um dem EU-Standard (DSGVO) Rechnung zu tragen und enthält im Wesentlichen keine Swiss Finishes. Damit schafft das Gesetz Rechtssicherheit für Schweizer Unternehmen, welche sich (auch) an die Bestimmungen der DSGVO halten müssen. **Der Entwurf der Verordnung zum Datenschutzgesetz (E-VDSG) gefährdet die gewonnene Rechtssicherheit durch zahlreiche Regelungen, welche über diejenigen der DSGVO hinausgehen.** Wir bitten Sie, den Entwurf dahingehend zu überarbeiten, dass sämtliche Swiss Finishes und Widersprüche zum revDSG beseitigt werden. Die Verordnung hat sich auf Konkretisierungen des Gesetzes zu beschränken und darf insbesondere nicht Regelunge aufzustellen, welche bewusst nicht in das Gesetz aufgenommen wurden (z.B. Art. 16 E-VDSG).

Unsere nachfolgenden Anregungen und Formulierungsvorschläge in Bezug auf einzelne Artikel des Entwurfs mögen Ihnen bei der Überarbeitung dienen. Alle aufgeführten Punkte sind aus unserer Sicht grundsätzlich zwingend zu berücksichtigen (Prio 1: rot, Prio 2: orange, Prio 3: gelb).

Bei allfälligen Rückfragen stehen wir Ihnen gerne zur Verfügung

Freundliche Grüsse

Prof. Dr. iur. Cornelia Stengel
Geschäftsführerin

MLaw Luca Stäuble
Stv. Geschäftsführer

Artikel	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag
Generell	Entgegen ihrer Natur als reine ***Ausführungs***verordnung zum Datenschutzgesetz enthält die E-VDSG Regelungen, welche über eine blosse Konkretisierung des revDSG hinausgehen.	Die VDSG hat ausschliesslich die Konkretisierung des revDSG zum Zweck (vgl. Erläuterungen, S. 9). Sie darf darüber hinaus keine zusätzlichen eigenen Regelungen vorsehen. Dies führte zu einer eigentlichen Parallelgesetzgebung.	Konsequente Streichung aller mit dem E-VDSG eingeführten **Swiss Finishs** (vgl. nachfolgend). Ergänzung der Titel in der Verordnung mit einer Verweisung auf die entsprechende gesetzliche Grundlage. Z.B.: „Art. 1 Grundsätze (Art. 8 Abs. 3 DSG)“
	Die zusätzlich aufgestellten Regelungen entbehren nicht nur einer Rechtsgrundlage im Gesetz, wo der Gesetzgeber teilweise bewusst anders entschieden hat, sondern gehen auch über das Niveau der DSGVO hinaus. Diese **Swiss Finishs** stehen aber im Widerspruch zur expliziten Zielsetzung des Gesetzgebers und auch des BJ, wonach Kompatibilität mit der DSGVO geschafft werden sollte (Erläuterungen, S. 10).	Wie das BJ in den Erläuterungen (S. 10) selbst ausführt, soll durch Kompatibilität mit der DSGVO Rechtssicherheit für Unternehmen geschaffen werden, welche sich an die DSGVO halten. Das gelingt freilich nicht, wenn die VDSG gegenüber dem revDSG (neue) **Swiss Finishs** einführt. Im Gegenteil, damit sind Doppelspurigkeiten und Widersprüche vorprogrammiert.	

1	Berücksichtigung des Implementierungsaufwands statt der -kosten als Kriterium aufnehmen.	Die Erläuterungen zur Berücksichtigung der Implementierungskosten als Kriterium bei der Beurteilung der Angemessenheit sind u.E. unpräzise (vgl. Erläuterungen, S. 16). Entgegen diesen Ausführungen sind die Implementierungskosten gemäss E-VDSG 1 I b bei der Beurteilung der Frage, ob eine Massnahme angemessen ist, zu berücksichtigen, und nicht erst, wenn es darum geht, sich für eine von mehreren angemessenen Massnahmen zu entscheiden. Zudem ist nicht allein auf die Implementierungs*kosten*, sondern generell auf den Implementierungs*aufwand* abzustellen. Das sollte in der Verordnung entsprechend präzisiert werden.	1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a.–c. […]; d. Implementierungs~~kosten~~*aufwand*. ~~2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.~~ **Eventualiter:** 1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a.–c. […]; d. Implementierungs~~kosten~~*aufwand*. 2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessene~~n~~*r* ~~Abständen~~ *Weise* zu überprüfen.
	Streichung der Pflicht zur Überprüfung in angemessenen Abständen. **Eventualiter:** Pflicht zur Überprüfung der Massnahmen in angemessener *Weise*	Die Pflicht zur Überprüfung in angemessenen Abständen nach VDSG 1 II hat keine Grundlage im revDSG. **Eventualiter:** Wenn, dann sind die Massnahmen infolge risikobasierten Ansatzes nicht in angemessenen *Abständen*, sondern vielmehr in angemessener *Weise* zu überprüfen. Denn die Frage, ob eine Kontrolle nötig ist, hängt insbesondere davon ab, ob sich die Risiken geändert haben. Zeitliche Aspekte sind irrelevant.	

3	Die Protokollierungspflicht nach VDSG 3 ist zu streichen. **Eventualiter:** Einschränkung auf Fälle, wo ohne Protokollierung nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden (vgl. auch geltender Art. 10 Abs. 1 VDSG).	Die Protokollierungspflicht nach VDSG 3 hat keine Grundlage im revDSG und widerspricht dem risikobasierten Ansatz. Auch „hohen" Risiken ist mit den im Einzelfall *adäquaten Massnahmen* zu begegnen. Die DSGVO sieht keine Protokollierungspflicht vor. Es handelt sich daher um einen **Swiss Finish**. Auf einer Dokumentationspflicht, wie sie im VE-DSG vorgesehen war, wurde aufgrund der Eingaben in der Vernehmlassung verzichtet bzw. sie wurde durch die Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen ersetzt. Diese geht weiter als die bisherige Pflicht zur Anmeldung der Datensammlung beim EDÖB. Es müssen neu alle Bearbeitungen in einem Verzeichnis aufgeführt sein. Es nicht erforderlich, an der Protokollierungspflicht festzuhalten. Die Einführung der Protokollierungspflicht als Teil der Datensicherheit hätte stossende Auswirkungen: Falls trotz gegebenen Voraussetzungen keine DSFA durchgeführt wird, so hat dies gemäss revDSG *keine* Sanktion zur Folge. Wird hingegen eine DSFA durchgeführt, aber in der Folge gegen die allfällige Protokollierungspflicht (als Teil der Datensicherheit) verstossen, so ist das sanktionsbedroht. Der Verantwortliche hat die vorgängig Stellungnahme des EDÖB einzuholen, wenn sich aus der DSFA ergibt, dass eine geplante Bearbeitung trotz Massnahmen ein hohes zur Folge hat. Der EDÖB kann dem Verantwortlichen bei etwaigen Einwänden (angemessene) ebenfalls Massnahmen vorschlagen.	**Streichung von VDSG 3**, zumindest für den Privatbereich. **Eventualiter:** 1 Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht *und kann sonst nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden,* protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. 2 […] 3 […] 4 […]

4	Die Pflicht zur Erstellung eines Reglements nach VDSG 4 ist zu streichen. **Eventualiter:** Falls an dieser Regelung festgehalten werden sollte, müsste zumindest präzisiert werden, dass die Angaben gemäss Abs. 2 einzig in Bezug auf Bearbeitungen gemacht werden müssen, welche unter Art. 1 Abs. 1 lit. a und/oder b fallen.	Die Pflicht zur Erstellung eines Reglements nach VDSG 4 I hat keine Grundlage im revDSG und widerspricht dem risikobasierten Ansatz. Auch „hohen" Risiken ist mit den im Einzelfall *adäquaten* Massnahmen zu begegnen. Die DSGVO sieht keine Pflicht zur Erstellung eines Reglements vor. Es handelt sich daher um einen **Swiss Finish**. Auf eine Dokumentationspflicht, wie sie im VE-DSG vorgesehen war, wurde aufgrund der Eingaben in der Vernehmlassung verzichtet bzw. sie wurde durch die Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen ersetzt. Diese geht weiter als die bisherige Pflicht zur Anmeldung der Datensammlung beim EDÖB. Es müssen neu alle Bearbeitungen in einem Verzeichnis aufgeführt sein. Es nicht erforderlich, an der praxisfernen Pflicht zur Erstellung eines Reglements festzuhalten.	**Streichung von VDSG 4**, zumindest für den Privatbereich.

6	Unklar, was die Ausführungen auf S. 24 der Erläuterungen zu den Anforderungen an den Inhalt des ADV gemäss Art. 22 Abs. 3 DSGVO bezwecken, zumal diese in Art. 6 E-VDSG nicht vorgesehen sind.	Diese Ausführungen suggerieren, dass der ADV gemäss VDSG 6 den inhaltlichen Anforderungen der DSGVO genügen müsse. Hierfür findet sich indes keine gesetzliche Grundlage. Auch die E-VDSG enthält keine inhaltlichen Vorgaben.	Klarstellung im Erläuterungsbericht, dass die VDSG – anders als die DSGVO – keinen Mindestinhalt an den ADV vorschreibt.
	Streichung der Pflicht zur Sicherstellung einer vertrags- oder gesetzesgemässen Bearbeitung.	„Sicherstellung" der vertrags- und gesetzesgemässen Bearbeitung ist nicht möglich. Analog DSGVO 28 I kann der Verantwortliche nur, aber immerhin verpflichtet werden, nur Auftragsbearbeiter zu beauftragten, welche durch angemessene Massnahmen die Bearbeitung im Einklang mit den Anforderungen des revDSG und den Schutz der Rechte der Betroffenen gewährleisten.	1 Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. ~~Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.~~ *Er arbeitet nur mit Auftragsbearbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen so durchgeführt werden, dass die Bearbeitung im Einklang mit den Anforderungen der Schweizer Datenschutzgesetzgebung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.* 2 ~~Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.~~ 3 Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich *oder in einer anderen Form, die den Nachweis durch Text ermöglicht,* genehmigt hat.
	Streichung von Abs. 2, weil der Auslandtransfer separat geregelt ist.	Abs. 2: Auslandtransfers sind separat geregelt (E-VDSG 8), weshalb für diese Regelung keine Notwendigkeit besteht. Sollte an dieser Regelung festgehalten werden, so wäre im letzten Satz zu präzisieren, dass „andernfalls ein geeigneter Datenschutz gemäss Art. 16 Abs. 2 revDSG zu gewährleisten ist."	
	Präzisierung des Begriffs „schriftlich", der auch „in Text nachweisbare Formen" umfasst.	Abs. 3: „Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	

10	Der Empfänger kann nicht verpflichtet werden, „die schweizerischen Datenschutzvorschriften“ einzuhalten. Das ist im Erläuterungsbericht klarzustellen.	Im Erläuterungsbericht (S. 28) ist festgehalten, dass der Empfänger verpflichtet werden müsse, „die schweizerischen Datenschutzvorschriften“ einzuhalten. Das ist unzutreffend; er muss die Standardklauseln einhalten, nicht jedoch Schweizer Datenschutzrecht. So verlangt auch E-VDSG 6 II, dass der Auftragsbearbeiter „gleichwertige“ Bestimmungen einhalten muss.	Klarstellung im Erläuterungsbericht, dass der Empfänger nicht verpflichtet werden muss, „die schweizerischen Datenschutzvorschriften“ einzuhalten.
	Ersatz des Begriffs „Sicherstellung“ durch „darauf hinwirken“.	Der Exporteur kann nicht „sicherstellen“, dass der Empfänger die Standarddatenschutzklauseln beachtet; er kann nur, aber immerhin darauf hinwirken.	1 Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um ~~sicherzustellen~~ *darauf hinzuwirken*, dass die Empfängerin oder der Empfänger diese beachtet. *Die Angemessenheit der Massnahmen richtet sich nach den Umständen im konkreten Fall und dem Stand der Technik.* 2 […]
	Präzisierung, dass sich die Angemessenheit der geforderten Massnahmen nach den Umständen im konkreten Einzelfall richte und die Anforderungen insb. dann höher seien, wenn es sich um besonders schützenswerte Personendaten handle.	Dies ist in den Erläuterungen (S. 28) unter Hinweis auf das BJ entsprechend festgehalten und sollte zur Klarstellung auch in die Verordnung einfliessen. Der risikobasierte Ansatz bei der Beurteilung von Datentransfers in Länder ohne angemessenen Datenschutz auf Grundlage der SCC ist zu bejahen. Allerdings ist dieser Ansatz mit Blick auf die Praxishinweise der EU-Behörden keinesfalls selbstverständlich. Entsprechend bedarf es einer Klarstellung in der Verordnung zur Schaffung von Rechtssicherheit.	
NEU	Präzisierung des räumlichen Anwendungsbereichs des revDSG (Auswirkungsprinzip, Art. 3 I):	Gemäss revDSG 3 I gilt das Gesetz für Sachverhalte, die sich in der Schweiz auswirken auch wenn sie im Ausland veranlasst werden. Weder das Gesetz noch die Verordnung halten fest, ob an die Auswirkungen weitere Anforderungen zu stellen sind. Eine solche qualifizierte Auswirkung (Spürbarkeit) ist erforderlich, um Übertreibungen bei der extraterritorialen Anwendung des Schweizer Datenschutzrechts vorzubeugen. Hierzu ist eine Regelung analog zum Marktortprinzip gemäss DSGVO aufzunehmen.	*Folgende Sachverhalte, die im Ausland veranlasst werden, wirken sich in der Schweiz aus:* a. *das Angebot von Waren oder Dienstleistungen gegenüber betroffenen Personen in der Schweiz;* b. *die Beobachtung des Verhaltens von betroffenen Personen, soweit ihr Verhalten in der Schweiz erfolgt.*

13	Richtigstellung, dass keine „Basisinformationen“ auf der ersten Kommunikationsstufe mitgeteilt werden müssen.	Das revDSG sieht nicht vor, dass die Betroffenen die „wichtigsten Informationen“ auf der „ersten Kommunikationsstufe“ erhalten müssen (vgl. aber Erläuterungen, S. 30). Vielmehr hält revDSG 19 I fest, die Information müsse „angemessen“ erfolgen. Daraus folgt, dass das die Mitteilung von den jeweiligen Umständen abhängig ist. Dabei sind auch Informationsinteresse und die Erwartungen des Betroffenen zu berücksichtigen: Während er damit rechnen mag, dass sich in einem Vertrag ein Hinweis auf den die Datenschutzerklärung findet, ist ein solcher auf Visitenkarten, E-Mails oder Briefpapier nicht üblich. Sollte sich eine Person dafür interessieren, kann ihr zugemutet werden, die Webseite des betreffenden Unternehmens zu konsultieren. Darum darf es nicht erforderlich sein, in Alltagssituationen – wie bei einer Terminvereinbarung, am Schalter – explizit auf die Datenschutzerklärung hinweisen zu müssen (s. Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 99). Zudem wäre ohnehin unklar, welches die „wichtigsten Informationen“ sind.	Richtigstellung im Erläuterungsbericht, dass den Betroffenen keine „Basisinformationen“ auf der ersten Kommunikationsstufe mitgeteilt werden müssen und dass auch das Informationsinteresse der Betroffenen im Einzelfall zu berücksichtigen ist.
	Streichung der gesetzlich nicht vorgesehenen Informationspflicht des Auftragsbearbeiters.	Der Auftragsbearbeiter hat gemäss revDSG keine Informationspflicht (vgl. revDSG 19). Eine solche kann nicht in der VDSG eingeführt werden.	**Streichung von Art. 13 VDSG** **Eventualiter:** ~~1~~ Der Verantwortliche ~~*und der Auftragsbearbeiter teilen*~~ *teilt* die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit. *Als leicht zugänglich gilt insbesondere die Information, welche auf der Webseite des Verantwortlichen abrufbar ist.* ~~2 Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~
	Streichung der unpräzisen Vorgaben für eine angemessene Information. Streichung der unklaren Anforderungen an Piktogramme.	Weil Piktogramme ohnehin nur ergänzend verwendet werden dürfen, sind daran keine zusätzlichen Anforderungen zu stellen. Zumal aufgrund der Erläuterungen nicht klar ist, was mit „maschinenlesbar“ gemeint ist.	

15	Die Informationspflicht bei der Bekanntgabe von Personendaten ist zu streichen.	Diese Informationspflicht entbehrt einer Grundlage im revDSG. Auf die Richtlinie (EU) 2016/680 (Schengen-RL) ist für den Privatbereich nicht abzustellen. Die DSGVO sieht keine entsprechend Pflicht vor. Eine Umsetzung ist nicht erforderlich und schafft einen **Swiss Finish**. Der Auftragsbearbeiter ist gemäss revDSG wie bereits erwähnt nicht Adressat der Informationspflicht. Keine Notwendigkeit: Der Verantwortliche hat bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten.	**Streichung von Art. 15.**
16	Die Informationspflicht über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten ist zu streichen.	Diese Informationspflicht entbehrt einer Grundlage im revDSG. Diese Pflicht wurde im Vorentwurf des DSG vorgeschlagen, im Rahmen der Vernehmlassung jedoch wieder gestrichen. Sie darf entsprechend nicht über die VDSG wieder eingeführt werden. Keine Notwendigkeit: Der Verantwortliche hat bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten.	**Streichung von Art. 16.**

18	Analog DSGVO 35 IV soll der EDÖB eine Liste erstellen und publizieren, welche Bearbeitungen enthält, für die eine bzw. keine DSFA zu erfolgen hat. Alternativ oder kumulativ sind Kriterien zu nennen, wonach ermittelt werden kann, ob eine DSFA durchzuführen ist oder nicht. „Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	Ohne Kriterien und/oder Liste mit Beispielen von Bearbeitungen, die eine DSFA erfordern bzw. nicht erfordern, besteht eine grosse Rechtsunsicherheit.	*1 Der Beauftragte erstellt eine Liste mit Bearbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Er kann zusätzlich eine Liste mit Bearbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.* *2* Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich *oder in einer anderen Form, die den Nachweis durch Text ermöglicht,* festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~
	Die Aufbewahrungsfrist ist zu streichen.	Die Dokumentationspflicht gemäss VDSG 18 entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Zudem besteht der Anreiz, der Dokumentationspflicht nicht nachzukommen, da diese – im Gegensatz zu einer Verletzung der Datensicherheit – nicht strafbar ist. Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelungen einen **Swiss Finish** darstellen.	
	Der Begriff der Schriftlichkeit ist zu präzisieren.	„Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	

19	Die Auslegung des Begriffs „voraussichtlich“ ist falsch und zu korrigieren.	„Voraussichtlich“ heisst nicht, dass „in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen kann, eine Meldung erfolgen muss“ (so die Erläuterungen, S. 32). Der Begriff „voraussichtlich“ setzt vielmehr voraus, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko führt.	Richtigstellung im Erläuterungsbericht, dass in Fällen, wo das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, nicht gemeldet werden muss, sondern nur dann, wenn die Verletzung der Datensicherheit **höchstwahrscheinlich** zu einem hohen Risiko führt.
	Streichung der in der Verordnung gegenüber dem Gesetz zusätzlich eingeführten Mindestangaben bei einer Meldung einer Verletzung der Datensicherheit.	Gemäss revDSG 24 II hat der Verantwortliche in der Meldung einer Verletzung der Datensicherheit „mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen zu [nennen]“. Die E-VDSG sieht weitere Mindestangaben vor. Die DSGVO sieht keine Angabe von Zeitpunkt und Daher der Verletzung vor. Es handelt sich daher um einen **Swiss Finish**.	1 Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit: a. die Art der Verletzung; ~~b. soweit möglich den Zeitpunkt und die Dauer;~~ ~~c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;~~ ~~d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;~~ e.-g. […] 2 […] *3* ~~Der~~ *Falls der* Verantwortliche *verpflichtet ist, die* ~~teilt den~~ betroffenen Personen *zu informieren, so teilt er ihnen* in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit. 4 […] ~~5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.~~
	Streichung der über das Gesetz hinausgehenden generellen Pflicht, die betroffene Person zu informieren.	E-VDSG 19 II geht über revDSG 20 IV hinaus. Während das Gesetz eine Information der betroffenen Person nur vorschreibt, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt, sieht die Verordnung vor, dass der Verantwortliche den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mitteilt.	
	Streichung der gesetzlich nicht vorgesehenen Dokumentationspflicht nach VDSG 19 V.	Dokumentationspflicht nach VDSG 19 V entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie nach der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor. Es handelt sich daher um einen **Swiss Finish**. Falls an der Dokumentationspflicht festgehalten werden sollte, ist zu präzisieren, dass nur meldepflichtige Verletzungen aufzubewahren sind.	

20	Die Auskunftserteilung sollte nicht nur schriftlich, sondern auch in einer anderen durch Text nachweisbaren Form möglich sein.	In den Erläuterungen (S. 34) wird festgehalten: „Es kann hier ferner präzisiert werden, dass zur schriftlichen Form auch die elektronische Form gehört." Diese Präzisierung ist in die Verordnung aufzunehmen.	1 […] 2 Die Auskunft wird in der Regel schriftlich *oder in einer Form, die den Nachweis durch Text ermöglicht,* erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat. 3-4 […] *5 Die betroffene Person hat keinen Anspruch auf Herausgabe von Dokumenten, selbst wenn diese Personendaten enthalten sollten.* ~~5 Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.~~
	Aufnahme der Präzisierung, dass der Begriff „Daten als solche" insbesondere auch eine Auskunft in aggregierter Form zulässt.	In den Erläuterungen (S. 35) wird ausgeführt: „Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Die mündliche Mitteilung von Informationen, zum Beispiel am Telefon, ist ebenfalls möglich, sofern die betroffene Person eingewilligt hat." Es besteht im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten bzw. Unterlagen. Vielmehr ist die Mitteilung nach entsprechender Debatte vom Gesetzgeber bewusst beschränkt worden auf die bearbeiteten Personendaten „als solche" (revDSG 25 II b). Damit soll namentlich auch die Auskunft in aggregierter Form ermöglicht werden. Dies sollte zwecks Präzisierung in der Verordnung verankert werden.	

	Dokumentationspflicht nach VDSG 20 V ist zu streichen.	Dokumentationspflicht nach VDSG 20 V entbehrt einer gesetzlichen Grundlage(vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen **Swiss Finish** darstellen. Die Regelung ist ferner unnötig, da aufgrund der Beweislast ohnehin im Interesse des Verantwortlichen mit Dokumentation den Nachweis erbringen zu können.	
22	Der Fristenbeginn ist zu präzisieren.	Präzisierung erforderlich: Wenn aus dem Auskunftsbegehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.	1 Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen. *Wenn aus dem Begehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.* 2 […]
23	Erhöhung der Beteiligung an den Kosten für eine Auskunftserteilung.	Eine wesentliche Erhöhung der Beteiligung des Betroffenen ist angezeigt, weil der geltende Betrag von CHF 300.00 regelmässig in keinem Verhältnis zum Aufwand steht.	1 […] 2 Die Beteiligung beträgt maximal *5'000.00* Franken. 3 […]

24	Klarstellung, dass „Datenportabilität" kein Zwang zu standardisierten Datenbearbeitungssystemen beinhaltet.	Die „Datenportabilität" wurde erst im Rahmen der parlamentarischen Debatte eingeführt. Entsprechend enthält die Botschaft keine Ausführungen dazu. Die Verordnung muss hier Konkretisierungsarbeit leisten.	*1 Das Recht der betroffenen Person, sie betreffende Personendaten vom Verantwortlichen heraus zu verlangen oder durch diesen an einen anderen Verantwortlichen übertragen zu lassen, begründet für den Verantwortlichen nicht die Pflicht, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten.* *2* […]
26	Es ist zu präzisieren, dass sich die allfällige Pflicht eines KMU zur Führung eines Verzeichnisses nicht auf sämtliche Bearbeitungen erstreckt, sondern auf diejenigen Bearbeitungen beschränkt ist, welche die Voraussetzung(en) triggern.	Der Bundesrat hat gemäss revDSG 12 V Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses vorzusehen für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und deren Datenbearbeitung ein „geringes Risiko" mit sich bringt. Gemäss E-VDSG 26 bedeutet ein geringes Risiko, dass weder „umfangreich besonders schützenswerte Personendaten bearbeitet" werden noch „ein Profiling mit hohem Risiko durchgeführt" wird. Alle anderen Bearbeitungen bringen im Umkehrschluss ein geringes Risiko mit sich. Durch Präzisierung, dass sich die Pflicht zur Führung eines Verzeichnisses ausschliesslich auf diejenigen Bearbeitungen erstreckt, welche die Voraussetzung triggern, kann sowohl dem Schutz der betroffenen Personen als auch den Bedürfnissen der KMU angemessen Rechnung getragen werden (vgl. auch das Positionspapier des EDSA zu Art. 30 Abs. 5 DSGVO).	1 Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. […] b. […] *2 Ist eine Voraussetzung nach Abs. 1 Bst. a und/oder b erfüllt, so ist die Verzeichnispflicht auf diejenige bzw. diejenigen Bearbeitungen beschränkt, welche dieser bzw. diesen Voraussetzung bzw. Voraussetzungen zugrunde liegen.* *3 Das Bearbeitungsverzeichnis ist schriftlich, oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu führen.*
	Es ist ferner zu präzisieren, dass das Verzeichnis nicht schriftlich, sondern auch in anderer Form, die den Nachweis durch Text ermöglicht, z.B. elektronisch, geführt werden kann.	Damit ist klargestellt, dass das Verzeichnis auch elektronisch geführt werden kann.	

…

scienceindustries
Wirtschaftsverband
Chemie Pharma Life Sciences

Nordstrasse 15
Postfach
8021 Zürich
Schweiz

T +41 44 368 17 11
info@scienceindustries.ch

Frau Bundesrätin
Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
jonas.amstutz@bj.admin.ch

Zürich, 13. Oktober 2021

Stellungnahme von scienceindustries zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz

Sehr geehrte Frau Bundesrätin

Wir danken für die Möglichkeit zur Stellungnahme im Rahmen der am 23. Juni 2021 eröffneten Vernehmlassung zur eingangs erwähnten Verordnung.

scienceindustries ist der Schweizer Wirtschaftsverband Chemie Pharma Life Sciences. Sie vertritt die wirtschaftspolitischen Interessen von weit über 250 in der Schweiz tätigen Unternehmen aus genannten und verwandten Branchen. Unsere Mitgliedsunternehmen sind mittlerweile für mehr als 50% aller Schweizer Exporte verantwortlich. Entsprechend international gestaltet sich deren Datenverarbeitung aus. scienceindustries setzt sich daher für einen modernen und zweckmässigen Datenschutz ein, der die Innovationskraft unseres Standorts nicht behindert. Ein administrativ tragbares Vorgehen im Rahmen der internationalen Entwicklungen ist dabei zentral.

Im Rahmen der parlamentarischen Beratung zum revidierten Datenschutzgesetz wurden Schweizer Besonderheiten grösstenteils vermieden. Der vorliegende Entwurf der totalrevidierten Verordnung zum DSG (E-VDSG) folgt nun leider der vom Parlament im revDSG vorgegeben Stossrichtung nicht. Er verschärft wesentliche Punkte des Gesetzes, ist inhaltlich nicht ausreichend präzise und unnötig restriktiv. Statt das revDSG im Sinne von Ausführungsvorschriften zu konkretisieren, sieht der Entwurf der Verordnung eine Reihe von bürokratischen Zusatzvorschriften mit vielen Swiss Finishes vor, die keine Grundlage im Gesetz finden.

Der **Entwurf** muss daher unter Berücksichtigung des revDSG und insbesondere der politisch intensiv geführten Diskussion, welche zu zahlreichen Kompromissen im Parlament geführt hat, noch einmal **stark überarbeitet** werden. Der vorliegende Entwurf wird von scienceindustries klar kritisiert und in dieser Form abgelehnt, da er keine Grundlage für einen zweckmässigen, zukunftsgerichteten Datenschutz darstellt. Nachfolgend führen wir die für **scienceindustries wichtigsten Anliegen** auf, wobei vorab festgehalten werden soll, dass scienceindustries die **ausführliche Stellungnahme von economiesuisse vollumfänglich unterstützt** und hier auch auf diese verweist.

Bearbeitungsreglement von privaten Personen

scienceindustries beantragt die **ersatzlose Streichung von Art. 4 E-VDSG**. Die Regelung wurde im Wesentlichen aus Art. 11 der geltenden VDSG übernommen. Schon jene Bestimmung blieb aber insofern «toter Buchstabe», als es ein solches «Bearbeitungsreglement» in dieser Form in der operativen Praxis von

Unternehmen nicht gibt. Vielmehr werden die zahlreichen notwendigen Regelungen gemäss bewährter Usanz in einem ganzen Paket von sich gegenseitig ergänzenden Weisungen samt dazugehörigen Prozessen und Listen mit Aufgaben, Kompetenzträgern und Verantwortlichkeiten abgebildet. Diese sind sehr viel wirkungsvoller als ein starres Reglement. Das in der E-VDSG vorgesehene Bearbeitungsreglement kann die immer komplexeren Datenbearbeitungen in der Praxis nicht mehr sinnvoll abbilden. Diese Aufgabe übernimmt zu Recht das neu zu führende Verzeichnis der Bearbeitungstätigkeiten (Art. 12 revDSG).

Umso unverständlicher ist, dass die Regelung von Art. 4 E-VDSG weitgehend deckungsgleich mit den Anforderungen an das gemäss Art. 12 revDSG zu erstellenden Verzeichnis der Bearbeitungstätigkeiten ist, was unnötigerweise Rechtsunsicherheit und unnötigen Doppelaufwand produziert. Das revDSG sieht in Art. 12 bereits vor, dass die Datenverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten führen müssen. Dieses muss ähnliche Informationen enthalten wie das Bearbeitungsreglement. Mit der Einführung des Verzeichnisses macht ein zusätzliches Bearbeitungsreglement keinen Sinn. Dies umso mehr, als unsere Mitgliedsunternehmen überdies auch grenzüberschreitende Geschäfte betreiben und deshalb entsprechende Verzeichnisse nach Art. 30 DSGVO erarbeiten müssen. Verzeichnisse, welche für die DSGVO erstellt wurden, können für das Verzeichnis der Bearbeitungstätigkeiten nach Art. 12 revDSG mit Ergänzungen direkt übernommen werden. Demzufolge beantragt scienceindustries die ersatzlose Streichung von Art. 4 E-VDSG.

Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs

Aus Sicht von scienceindustries **muss Art. 8 in dessen Abs. 1 wie auch in Abs. 6 angepasst werden**, um klarzustellen, dass sich diese Regelung ausschliesslich an den Bund richtet. Der Wortlaut kann dahingehend missverstanden werden, dass die verantwortliche Stelle – und nicht der Bundesrat – die Angemessenheit in einem Empfängerstaat feststellen muss. Es muss klargestellt werden, dass sich dieser **Artikel nur an den Bundesrat richtet**, und dass dieser einzige kompetente Stelle wird, welche eine solche Positiv-Liste erlassen kann. Der EDÖB wird vom Bundesrat konsultiert, kann jedoch keine eigene Liste herausgeben. Die Aufgabe des EDÖB liegt neu lediglich darin, Empfehlungen/Assessmentvorgaben für den Datentransfer in Länder zu formulieren, die nicht auf der Positiv-Liste des Bundesrates sind. Zudem muss diese **Liste für alleinig verbindlich** erklärt werden.

Pflichten des Verantwortlichen

Die Informationspflicht gegenüber betroffenen Personen kann nur den Verantwortlichen treffen. Die vorgesehene Regelung in Art. 13 E-VDSG steht im diametralen Widerspruch zum neuen DSG (Art. 19 revDSG) und der DSGVO (Art. 13 und 14). In beiden Gesetzen trifft die Informationspflicht nur den Verantwortlichen. Der Auftragsbearbeiter soll und kann nicht informieren. Daher beantragt scienceindustries die **Streichung des Auftragsbearbeiters im Titel zu Kapitel 2 und in Art. 13 Abs. 1 E-VDSG**.

Information bei der Bekanntgabe von Personendaten

Art. 15 E-VDSG statuiert völlig neue, formale zusätzliche Modalitäten und Zusatzpflichten in Zusammenhang mit der Bekanntgabe von Daten an Dritte, welche strikt regelbasiert ohne Differenzierungsmöglichkeit in jedem Fall anwendbar sein sollen. Hierzu findet sich im revDSG **keine gesetzliche Grundlage**. Im Gegenteil hat das Parlament die Bekanntgabe von Personendaten an Dritte bereits auf Gesetzesstufe an verschiedenen Stellen ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt (vgl. namentlich Art. 16 ff. revDSG). Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen.

Die Regelung würde inhaltlich zu massiven Zusatzanforderungen bei jeder Art von Kommunikation in Zusammenhang mit Personendaten, z.B. bei jedem einzelnen E-Mail, führen. Damit würden an übliche und vernünftige Kommunikation, selbst solche ohne erkennbare datenschutzrechtliche Risiken, völlig überrissene Anforderungen gestellt. Dementsprechend finden sich auch im EU-Recht, auf welches sich der Erläuterungsbericht zu Unrecht beruft, keine solchen Pflichten für private Datenbearbeiter. Art. 15 E-VDSG

ist mithin ein für das wesentliche Regulierungsziel EU-Äquivalenz kontraproduktiver "Swiss Finish". Daher beantragt scienceindustries die **ersatzlose Streichung von Art. 15 E-VDSG**.

Information über die Berichtigung, Löschung und Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten

scienceindustries beantragt die **ersatzlose Streichung von Art. 16 E-VDSG**, denn diese Pflicht wurde im Rahmen der Vernehmlassung zum revDSG gestrichen und darf nun nicht über die VDSG wieder eingeführt werden. Zudem besteht keine Notwendigkeit, da der Verantwortliche bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten hat, ebenso wie die Empfänger von Personendaten.

Meldung von Verletzungen der Datensicherheit

scienceindustries beantragt die **ersatzlose Streichung** der gesetzlich nicht vorgesehenen **Dokumentationspflicht nach Art. 19 Abs. 5**. Zudem sieht die DSGVO keine solche Aufbewahrungspflicht vor, womit diese Regelung zusätzlich einen Swiss Finish darstellt.

Modalitäten nach Art. 20 E-VDSG

Die Dokumentationspflicht nach Art. 20 Abs. 5 E-VDSG entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung wieder einen Swiss Finish darstellt. Die Regelung ist ferner unnötig, da aufgrund der Beweislast ohnehin im Interesse des Verantwortlichen, mit Dokumentation den Nachweis erbringen zu können. scienceindustries beantragt daher die **ersatzlose Streichung von Art. 20 Abs. 5 E-VDSG**.

Ausnahmen von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeit

Nach Meinung der scienceindustries ist zu präzisieren, dass sich die allfällige Pflicht eines KMU zur Führung eines Verzeichnisses nicht auf sämtliche Bearbeitungen erstreckt, sondern auf diejenigen Bearbeitungen beschränkt ist, welche die Voraussetzung(en) auslösen. Daher gilt es die Bestimmung mit einem zweiten Absatz mit folgendem Wortlaut zu ergänzen:
[2] Ist eine Voraussetzung nach Abs. 1 lit. 1 und/oder b. erfüllt, so ist die Verzeichnispflicht auf diejenige bzw. diejenigen Bearbeitung(en) beschränkt, welche dieser bzw. diesen Voraussetzung(en) zugrunde liegen.

An dieser Stelle sei noch einmal wiederholt, dass wir für weitere, mitunter auch detailliertere Ausführungen auf die **Stellungnahme von economiesuisse verweisen, welche wir ausdrücklich unterstützen**.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Dr. Stephan Mumenthaler
Direktor

Jürg Granwehr
Bereichsleiter Pharma & Recht

Kontaktperson scienceindustries:
Jürg Granwehr
lic. iur. Rechtsanwalt
Bereichsleiter Pharma & Recht

T +41 44 368 17 28
Email: juerg.granwehr@scienceindustries.ch

Schweizer Dialogmarketing Verband

SDV DIALOGMARKETING VERBAND

Per Email:
jonas.amstutz@bj.admin.ch

Uzwil, 13. Oktober 2021

Vernehmlassung zur Revision der Datenschutzverordnung (VDSG)

Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, im Rahmen der Vernehmlassung über die Revision der Datenschutzverordnung (VDSG) Stellung zu nehmen.

Der SDV Schweizer Dialogmarketing Verband steht seit jeher in engem Austausch mit economiesuisse, dem Dachverband der Schweizer Wirtschaft und nimmt an der zugehörigen Fachgruppe "Datenschutz" teil. Der SDV unterstützt die Stellungnahme von economiesuisse zum VDSG sowie alle darin enthaltenen Anträge. Nachfolgende Anträge möchten wir hervorheben bzw. aus der Perspektive des SDV bekräftigen, da sich diese für die am SDV beteiligten Firmen bzw. Branchen in der Praxis besonders direkt und unnötig negativ auswirken.

Keine zusätzlichen Dokumentations- und Protokollierungspflichten

Art. 3 Protokollierung
Antrag: Ersatzlose Streichung des gesamten Artikels

Art. 4 Bearbeitungsreglement von privaten Personen
Antrag: Ersatzlose Streichung des gesamten Artikels

In der Stellungnahme von economiesuisse zur VDSG wird die Problematik der Artikel 3 und 4 treffend beschrieben und explizit auf die Problematik für KMU hingewiesen. Ein Grossteil der Mitglieder des SDV sind KMU. Zusätzlicher, gesetzlich verordneter, administrativer Aufwand ist insbesondere für KMU belastend, da er weder für das KMU selber noch für deren Kunden Nutzen stiftet. Es sollte daher mindestens vermieden werden, dass administrativen Pflichten unnötig detailliert (Protokollierung gemäss Art. 3) ausfallen oder gar doppelt erledigt werden müssen (Bearbeitungsreglement gemäss Art. 4 sowie das Verzeichnis der

SDV Schweizer
Dialogmarketing Verband
Postfach 445
9240 Uzwil

T 071 277 00 50

info@sdv-dialogmarketing.ch

www.sdv-dialogmarketing.ch
www.sdv-konsumenteninfo.ch
www.sdv-award.ch

Bearbeitungstätigkeiten gemäss Art. 12 revDSG). Der Umstand, dass viele KMU auf Grund der definierten Kriterien in Art. 3 Abs. 1 sowie Art. 4 Abs. 1 Lit. a und b nicht von den Regelungen betroffen wären, ändert nichts an der Grundhaltung zur Vermeidung von unnötigem, administrativem Aufwand.

Keine zusätzlichen Pflichten für Auftragsbearbeiter

Art. 13 Modalitäten der Informationspflichten
Antrag: Streichung des Auftragsbearbeiters

Art. 15 Information bei der Bekanntgabe von Personendaten
Antrag: Ersatzlose Streichung des gesamten Artikels

Im Dialogmarketing werden häufig auch kleinere Datenbearbeitungen durch dritte Dienstleiter (Auftragsbearbeiter) erledigt. So z.B. ein Datenabgleich oder die Produktion eines Mailings. Es ist in der Praxis in Bezug auf den Aufwand sowie insbesondere auf Grund der rechtlichen Risiken (Verletzungen der Informationspflicht sind strafbewehrt) nicht verhältnismässig, dass dem Auftragsbearbeiter dadurch eine Informations- oder Auskunftspflicht zukommt.

Keine zusätzlichen Informationspflichten

Art. 15 Information bei der Bekanntgabe von Personendaten
Antrag: Ersatzlose Streichung des gesamten Artikels

Art. 16 Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten
Antrag: Ersatzlose Streichung des gesamten Artikels

Die kontrollierte Weitergabe von Personendaten ist ein Geschäftszweck von verschiedenen Mitgliedern des SDV. Im Regelfall werden Daten den Empfängern für die einmaligen Verwendung (z.B. Adressierung eines Mailings) überlassen. Es ist somit nicht ersichtlich, weshalb eine spätere Information über die Berichtigung, Löschung oder Einschränkung an den Adressempfänger nötig sein sollte.

Freundliche Grüsse

Roger Muffler
Präsident SDV

Lukas Bühlmann
Vorstand SDV

SDV Schweizer
Dialogmarketing Verband
Postfach 445
9240 Uzwil

T 071 277 00 50

info@sdv-dialogmarketing.ch

www.sdv-dialogmarketing.ch
www.sdv-konsumenteninfo.ch
www.sdv-award.ch

senesuisse
Verband wirtschaftlich unabhängiger Alters- und Pflegeeinrichtungen Schweiz
Association d'établissements économiquement indépendants pour personnes âgées Suisse

Per E-Mail an:

jonas.amstutz@bj.admin.ch

Bern, 11. Oktober 2021

Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG);
Stellungnahme des Verbandes *senesuisse*

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Einladung zur Beteiligung an der Vernehmlassung.

Im Jahr 1996 wurde der Verband ***senesuisse*** gegründet. Seither vertritt er die Interessen und Anliegen von Leistungserbringern im Bereich der Alterslangzeitpflege. Mehr als 450 Betriebe mit über 25'000 Pflegeplätzen sind Mitglied. Diese Betriebe sind einerseits mit hochsensiblen Daten betraut und andererseits auf möglichst einfach umsetzbare Regelungen angewiesen, um ihre Arbeit in optimaler Qualität zu leisten.

In der vorliegenden Vernehmlassungsantwort nimmt ***senesuisse*** zu jenen Massnahmen Stellung, die einen direkten Bezug zur Tätigkeit der Mitgliederinstitutionen aufweisen, also in der Alterspflege tätigen Betrieben.

Rückmeldung zu den relevanten Bestimmungen der E-VDSG für die ambulanten und stationären Betriebe für Personen mit Unterstützungsbedarf

E-VDSG	Kommentar	Beantragte Um-/ Neuformulierung
Art. 1 Abs. 1	Die vorgeschlagene Umschreibung ist im Grundsatz zu begrüssen. Sie ergänzt und konkretisiert sinnvollerweise Artikel 8 Absatz 1 nDSG. Zu begrüssen ist, dass sie möglichst schlank und angesichts der stetigen technischen Entwicklungen flexibel, praxisnah und anwendungsfreundlich gehalten worden ist. Weil sie sehr allgemein formuliert ist, braucht es aber entsprechenden Deutungs- und Umsetzungshilfen für die Praxis.	- Es müssen seitens EDÖB möglichst bald Dokumente geschaffen werden, welche den Betrieben die Praxisumsetzung vereinfachen.
Art. 1 Abs. 2	Die Abstände zwischen den vorzunehmen Überprüfungen sollten präziser angegeben werden, sonst drohen Rechts-unsicherheit und Streitigkeiten. Was genau „angemessene Abstände“ sind, hängt selbstverständlich von den Besonderheiten des konkreten Anwendungsfalls ab (S. 17 im erläuternden Bericht: «[…] bei der Bestimmung der Massnahmen selbstredend die Umstände des Einzelfalls massgeblich [bleiben]»). Während die Datenbearbeiter inhaltlich grossen Freiraum für die Bestimmung ihrer konkreten Massnahmen brauchen, sollte zeitlich zumindest	[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen, jedoch mindestens einmal pro Jahr zu überprüfen.

Postfach Bahnhofplatz 2 CH 3011 Bern
Telefon 031 911 20 20 info@senesuisse.ch www.senesuisse.ch

	eine konkrete Anforderung gelten, um die Sicherheit zu gewährleisten. Als sinnvoll erscheint uns eine mindestens jährliche Überprüfung.	
Art. 2	Diese präzise Auflistung der Schutzziele macht Sinn: Sie stellt eine praxisorientierte ‚Gedächtnisstütze' für die Verantwortlichen und die Auftragsbearbeiter dar, was im Rahmen ihrer Konkretisierung zu berücksichtigen ist. Wichtig ist eine gute Anwendbarkeit in der Praxis (Seite 17 des Berichts: „In Anwendung der Verhältnismässigkeit sind ausgehend [… von dieser Auflistung der Schutzziele] die organisatorischen und technischen Massnahmen des Einzelfalls zu bestimmen."). Gleichzeitig zeigt diese Auflistung die Komplexität der Anforderungen an eine gesetzkonforme Datenbearbeitung und -sicherheit auf - mit dem damit verbundenen Aufwand. Aus diesem Grund ist eine möglichst konkrete und für Schweizer Betriebe auch unentgeltliche Unterstützung der Datenschutzverantwortlichen durch die zuständigen Behörden (insbesondere das EDÖB), vorzusehen. So können die Umsetzungskosten für Wirtschaft und Gesellschaft minimiert und angemessene Datensicherheit auf allen Ebenen geschaffen werden.	- Für eine optimale und kostengünstige Umsetzung ist darauf zu achten, dass Schweizer Unternehmen einen guten und kostengünstigen Zugang zum EDÖB erhalten (vgl. auch Art. 45 Abs. 2).
Art. 3	Welche „Massnahmen" im vorliegenden Rahmen berücksichtigt werden sollen und ob ein Risiko als hoch oder begrenzt eingeschätzt werden soll, dürfte in der Praxis oftmals schwierig zu beurteilen sein, denn Artikel 8 nDSG führt auch keine präziseren Anhaltspunkte über die Art der infrage stehenden Massnahmen. Dies entspricht zwar einer flexiblen, bedarfsorientierten und dem neusten technischen Stand angepassten Umsetzung des Datenschutzes, macht aber dessen Realisierung in der Praxis schwierig. In diesem Sinne ist die Präzisierung der Inhalte der Protokollierung (gemäss Abs. 3) an sich konsequent und kongruent. Sie weist aber einen hohen Detaillierungsgrad auf, der einen entsprechend hohen Umsetzungsaufwand, eine Unübersichtlichkeit und mögliche Verwechslungsrisiken mit sich bringt. Es ist festzustellen, dass gerade bei der *automatisierten* Bearbeitung von Personendaten die Anforderung einer detaillierten Protokollierung einen beträchtlichen Teil der Vorteile der Automatisierung beraubt: Der zeitliche und administrative Aufwand wird dadurch erheblich vergrössert. Trotzdem erscheint uns eine Protokollierung richtig, sofern keine anderen Massnahmen das gleiche Ziel mit weniger Aufwand erreichen können. *Antrag:* Alternativen zur Protokollierung als Massnahmen zum Datenschutz sollen im E-VDSG ausdrücklich vorgesehen und auch aufgezählt werden – wie etwa die physische/räumliche Sicherung der Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.	In Art. 3 Abs. 1 müssen Alternativen zur im Entwurf vorgesehenen (komplexen) Protokollierung – ausdrücklich vorgesehen und auch aufgezählt werden, namentlich Zugriffskontrollen, die physische/räumliche Sicherung der Daten, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.

Art. 4 Abs. 2	Weil in sehr vielen Fällen eine automatisierte Bearbeitung von besonders schützenswerten Personendaten erfolgt, sind die von dieser Bestimmung gestellten Anforderungen als zu aufwendig und vielfach unnötig zu qualifizieren. Sie bringen für die betroffenen Datenbearbeiter unangemessen hohe Kosten mit sich. Deswegen ist diese Auflistung zu kürzen: Die Buchstaben d, e und j sollen ersatzlos gestrichen werden, weil sie unnötige zusätzliche Anforderungen und Präzisierungen darstellen, die den administrativen Aufwand für die Betriebe verschärfen, ohne dass daraus ein entsprechender Nutzen entsteht. Buchstabe i soll gekürzt werden: Er weist einen Detaillierungsrad mit entsprechenden Umsetzungskosten auf, der in keinem vernünftigen Verhältnis zu seinem Nutzen steht. Hingegen werden Buchstaben a, b, c, f und g ausdrücklich begrüsst, da sie zentrale Massnahmen zur Gewährleistung der Datensicherheit darstellen. Ihre Einhaltung genügt, um dem Datenschutz gerecht zu werden. Auch Buchstabe h wird begrüsst, weil eine stets angestrebte Datenminimierung das beste Mittel darstellt, um sowohl den Schutz der Privatsphäre als auch die Verminderung des mit jeglichem Datenbearbeitung verbundenen administrativen Aufwands zu erreichen.	[2] Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. ~~zur internen Organisation~~; e. ~~zur Herkunft der Personendaten und zur Art ihrer Beschaffung~~; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den ~~Datenbearbeitungsverfahren, insbesondere den~~ Verfahren bei der Speicherung, ~~Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung,~~ Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. ~~zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.~~
Art. 4 Abs. 3	Wie gemäss obigem Antrag zu Art. 1 Abs. 2 sollten auch hier die zeitlichen Abstände zwischen den vorzunehmen Aktualisierungen präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Deswegen wird hier beantragt, dass die Aktualisierungen mindestens einmal jährlich stattfinden: Dieser Zeitabstand stellt eine präzise, zugleich realistische und daher auch anwendungsfreundlich Leitplanke dar.	[3] Die private Person muss das Reglement ~~regelmässig~~ in angemessenen Abständen, jedoch mindestens einmal pro Jahr, aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.

Art. 6 Abs. 2	Die in dieser Bestimmung gestellten Anforderungen an die Verantwortlichen betreffend dem DSG nicht unterstellten Datenbearbeiter sind offensichtlich zu hoch. Von einem Verantwortlichen kann vernünftigerweise nicht verlangt werden, dass er Kenntnis der vielen potenziell relevanten Gesetzesbestimmungen und der möglichen Abhilfe-Lösungen hat. Wenn schon ist es die Pflicht von Gesetzgeber und Verwaltung, den Datenschutz so auszugestalten, dass dieser – wo nötig und sinnvoll – überall für alle Betroffenen gleichermassen gilt. Diese Pflicht den einzelnen Verantwortlichen aufzubürden, wie der Bundesrat es vorschlägt, führt zu enormer Unsicherheit und Aufwand. Deswegen ist dieser Absatz ersatzlos zu streichen.	~~[2] Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen~~ ~~Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege~~ ~~sicherstellen.~~
Art. 8 Abs. 1	Aus der Formulierung dieser Bestimmung geht überhaupt nicht klar hervor, wer für die Beurteilung der Angemessenheit des Datenschutzes in einem anderen Staat zuständig ist. Aus dem erläuternden Bericht hingegen schon (S. 25 ff): Der Bundesrat ist zuständig. Der Klarheit halber sollte diese Zuständigkeit in Art. 8 E-VDSC eindeutig geregelt werden, sonst besteht das Risiko, dass sich private Akteure dafür verantwortlich halten – was ihren Aufwand erheblich erhöhen würde.	[1] Werden Personendaten ins Ausland bekanntgegeben, so müssen ~~bei der~~ anlässlich einer regelmässigen Beurteilung durch den Bundesrat, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden: […]
Art. 8 Abs. 3	Die Abstände zwischen den vorzunehmenden Beurteilungen sollen präziser angegeben werden. Deswegen wird auch hier beantragt, dass die Beurteilungen mindestens einmal jährlich stattfinden müssen.	[3] Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch, jedoch mindestens einmal pro Jahr, neu beurteilt.
Art. 9 Abs. 1	Die von Art. 9 E-VDSG gestellten Anforderungen erreichen ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Zwar sind diese Anforderungen für das Ziel des Datenschutzes konsequent, sie verursachen aber hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden. Nämlich Bst. b, c, g, h sowie i sind offensichtlich unnötig; Ihre Anwendung wäre unverhältnismässig aufwendig. Die anderen Bestimmungen genügen, um die «spezifischen Garantien» zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.	[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen die Datensicherheit mindestens die folgenden Punkte regeln: […] ~~b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen~~

		~~c. die Art und der Zweck der Bekanntgabe von Personendaten;~~ ~~[…]~~ ~~g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger;~~ ~~h. die Massnahmen zur Gewährleistung der Datensicherheit;~~ ~~i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;~~ […]
Art. 10	Wir begrüssen, dass der EDÖB eine Liste von Standard-Datenschutzklauseln veröffentlicht, um den Aufwand für die Betroffenen zu reduzieren und eine gewisse Vereinheitlichung der Schutzklauseln zu erreichen.	-
Art. 15	Bei der Anwendung dieser Bestimmung ist darauf zu achten, dass die Anforderungen an den Detaillierungsgrad der mit der Bekanntgabe von Personendaten verbundenen Informationen nicht zu umfangreich ausfallen soll. Meistens werden sich die zum Datenschutz benötigten Informationen aus den Daten oder den Begleitumständen selbst ergeben.	-
Art. 18	Nach unserer Einschätzung reicht es aus, wenn *nach Beendigung der Datenbearbeitung* (was bei entsprechenden Gerichtsverfahren bereits Jahre dauern kann) eine Aufbewahrung für ein Jahr statt zwei Jahre stattfindet.	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während ~~zwei Jahren~~ einem Jahr nach Beendigung der Datenbearbeitung aufbewahrt werden.
Art. 20	Die vorgesehene Dreifachlösung (schriftlich, mündlich oder durch Einsichtnahme an Ort und Stelle) erscheint als sehr sinnvoll. So kann für Menschen mit gewissen Krankheiten oder Beeinträchtigungen eine geeignete Lösung gefunden werden. Für gewisse Fälle, wie urteilsunfähige, an Demenz erkrankte oder weitere kognitiv behinderte Menschen dürfte die Anforderung in Abs. 3 kaum einzuhalten sein. Deshalb ist für diese Fälle eine Präzisierung aufzunehmen.	[3] Die Auskunft muss für die betroffene Person verständlich sein, soweit dies im Rahmen des kognitiven Zustands möglich ist.
Art. 22	Die Frist von 30 Tagen ab Eingang des Begehrens um Dateneinsicht erscheint uns als vernünftig. Es stellt sich	-

	einzig die Frage, ob nicht die Gerichtsferien berücksichtigt werden sollten (namentlich die Sommermonate und Weihnachten, wegen vieler Absenzen).	
Art. 23	Bei unverhältnismässig aufwändigen Auskunftserteilungen erscheint uns die auf 300 Franken angesetzte Obergrenze als viel zu tief. Wenn damit mehrere Arbeitstage an Aufwand anfallen, wäre nicht einmal ein Bruchteil der Kosten auf die Gesuchstellenden gedeckt. Der Betrag sollte – auch gerade als Schutz vor querulatorischen Begehren – auf mindestens 1'000 Franken erhöht werden, um tatsächlich abschreckend wirken zu können.	[1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. [2] Die Beteiligung beträgt maximal ~~300~~ 1'000 Franken.
Art. 25	Die Datenschutzgesetzgebung weist eine hohe Komplexität auf; deshalb sind ihre Anforderungen in der Praxis nicht immer einfach einzuhalten. Deswegen ist es sehr sinnvoll, Datenschutzberatende einzusetzen und die konkreten Modalitäten zu deren Einsatz im Sinne dieser Bestimmung festzulegen. Die Inhalte sind zu begrüssen, wie sie in dieser Bestimmung vorgeschlagen sind.	-
Art. 26 Bst. a + b	Die hier definierte und sehr sinnvolle Ausnahme einer Pflicht zur Führung eines Bearbeitungsverzeichnisses würde bei zahlreichen Betrieben nicht zur Anwendung kommen, weil • in vielen Fällen die Betriebe besonders schützenswerte Personendaten in grossem Umfang bearbeiten; • aus einer Interpretation von Art. 20 Abs. 4, Art. 26 Abs. 3, Art. 31 Abs. 2 Bst. b nDSG hervorgeht, dass Art. 26 eVSDG auch Betriebe mit weniger als 250 Mitarbeitenden angewendet werden soll, wenn sie einem Konzern zugehören, der insgesamt mindestens 250 Mitarbeitende beschäftigt. Um Rechtssicherheit zu gewährleisten und keinen unnötigen Aufwand für kleinere Betriebe (namentlich auch gerade im Gesundheitswesen) zu schaffen, ist eine Anpassung wichtig. Während wir die Unterstellung von Teilen der Konzerne nachvollziehen können, erscheint uns die «Bearbeitung von besonders schützenswerten Daten in grossem Umfang» als zu wenig präzise Konkretisierung. Wir beantragen deshalb eine Präzisierung, was unter «grossem Umfang» zu verstehen ist, nach unserer Ansicht wäre die Schwelle etwa bei 1000 Datensätzen festzusetzen. Diesfalls erhält auch die Führung eines Verzeichnisses aber auf freiwilliger Basis mehr Gewicht, sie kann insbesondere bei regelmässiger Bearbeitung von Personendaten eine nützliche und einfache Tätigkeitsunterstützung darstellen: Dadurch können das Beibehalten eines Überblicks der Bearbeitungstätigkeiten und auch die Einhaltung anderer Verpflichtungen erleichtert werden.	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. Es werden umfangreich (mindestens 1000 Datensätze) besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.

Art. 45 Abs. 2	Aus unserer Sicht ist absolut unverständlich, warum eine nationale Behörde für die Dienstleistung im Bereich des der ganzen Bevölkerung dienenden Datenschutzes solch hohe Kostensätze von 150 bis 350 Franken verlangen soll. Dies schreckt geradezu ab, diese sinnvollen Dienstleistungen zu beziehen, welche einer guten Umsetzung der Gesetzgebung dienen. Es ist unverständlich, dass für die Dienstleistungen der Verwaltung solche Preise wie bei spezialisierten Anwaltskanzleien verrechnet werden. Als ganz besonders stossend empfinden wir solche Honorare im Bereich der nach KVG zugelassenen Leistungserbringer. Bei diesen Gesundheitsbetrieben handelt es sich um Institutionenen, bei welchen der Datenschutz wegen hoch sensibler Daten besonders wichtig ist. Es wäre falsch, diese mit hohen Stundensätzen vom Bezug der sinnvollen Unterstützung seitens EDÖB abzuschrecken. Diese Betriebe sind denn mit den neuen Regelungen auch besonders stark herausgefordert und eine gute Umsetzung ist im Interesse der Behörden und der Bevölkerung. Diese Belastung ist umso fragwürdiger, als die öffentliche Hand im Endeffekt und in vielen Fällen, die dadurch verursachten Defizite ausgleichen soll: Mit einer Hand wegnehmen, was mit der anderen gegeben wird, macht betriebswirtschaftlich keinen Sinn und verursacht einen sinnlosen administrativen Aufwand. Die Zutrittsschwelle zum EDÖB ist niedrig zu halten, ganz besonders auch zur Überprüfung der Angemessenheit von Kodizes (Art. 59 Abs. 1 Bst. a nDSG) oder die Genehmigung von Standarddatenschutzklauseln (Art. 59 Abs. 1 Bst. b nDSG). Im Sinne einer rechtmässigen Umsetzung der komplexen neuen Datenschutzgesetzgebung sollte das Anrufen des EDÖB nicht durch das Erheben von Gebühren entgegengewirkt werden. Ganz besonders für den Bereich der Gesundheitsbetriebe muss deshalb eine Ausnahme geschaffen werden, welche vernünftige Stundenansätze vorsieht.	[2bis] Für Leistungserbringer nach Art. 35 Abs. 2 KVG wird auf die Erhebung von Kosten verzichtet. Alternativ: [2bis] Für Leistungserbringer nach Art. 35 Abs. 2 KVG gilt ein Stundenansatz von 50 bis 100 Franken.

Wir danken Ihnen für die Kenntnisnahme und Berücksichtigung unserer Stellungnahme.

Mit freundlichen Grüssen
senesuisse

Christian Streit
Geschäftsführer

Schweizer Fleisch-Fachverband
Union Professionnelle Suisse de la Viande
Unione Professionale Svizzera della Carne

Sihlquai 255, 8005 Zürich
info@sff.ch
Tel. +41 (0)44 250 70 60
Fax +41 (0)44 250 70 61

Postanschrift/Adresse postale/Indirizzo postale:
Postfach, 8031 Zürich

Eidgenössisches Justiz- und
Polizeidepartement
Bundeshaus West
3003 Bern

Per E-Mail versandt an:
jonas.amstutz@bj.admin.ch

Zürich, 8. September 2021 / ze

Vernehmlassungsantwort

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

Wir beziehen uns auf die Eröffnung des Vernehmlassungsverfahrens bezüglich der im Betreff erwähnten Verordnung zum Bundesgesetz über den Datenschutz (VDSG) und erlauben uns, Ihnen unsere nachfolgende Vernehmlassungsantwort einzureichen.

Der Schweizer Fleisch-Fachverband (SFF) ist die Branchenorganisation für die fleischverarbeitende Branche, die rund 24'000 Mitarbeitende umfasst. Dem SFF als Arbeitgeberverband sind knapp 1'000 Mitglieder angeschlossen, darunter kleine gewerbliche Betriebe bis hin zu Grossbetrieben. Zudem ist der SFF mit verschiedenen weiteren sogenannten Selbsthilfeorganisationen in den Bereichen Versicherung, Sozialversicherung, berufliche Vorsorge, Ausbildung und Treuhanddienstleistungen für unsere Branche verbunden. Aufgrund der dadurch anfallenden datenschutzrelevanten Tätigkeiten, insbesondere im Bereich Mitgliederadministration sowie Austausch von Personendaten zwischen dem SFF und den obengenannten Selbsthilfeorganisationen, ist der SFF von der Totalrevision der VDSG direkt betroffen. Basierend auf dieser direkten Betroffenheit erlauben wir uns, Ihnen in diesem Vernehmlassungsverfahren unsere Einschätzung zukommen zu lassen.

I. Allgemeine Bemerkungen

Unsere Vernehmlassungsantwort beschränkt sich auf Anmerkungen zu Artikeln, die von uns kritisch beurteilt werden. Der SFF verzichtet auf allgemeine oder zustimmende Ausführungen zu den einzelnen Artikeln. Grundsätzlich sei jedoch angemerkt, dass der SFF die Totalrevision der VDSG in den Grundzügen befürwortet, dies vor allem auch, weil ein verbesserter Datenschutz die Digitalisierung stärkt. Gerade während der noch immer andauernden Corona-Pandemie wurde deutlich, welchen Mehrwert ein gutes Digitalisierungsniveau darstellt. Die Digitalisierung wird zudem in den nächsten Jahren einen immer wichtigeren Stellenwert einnehmen und ein entscheidendes Element wirtschaftlichen Fortkommens der Schweiz sein. Ein weiterer wesentlicher Aspekt der Totalrevision der VDSG ist, dass die gesamtwirtschaftliche Auswirkung dieser Revision eine elementare Voraussetzung dafür ist, dass das derzeit laufende Evaluationsverfahren der Schweiz durch die Europäische Kommission in der Beibehaltung des Angemessenheitsbeschlusses der EU endet, damit der Wirtschaftsstandort und die Wettbewerbsfähigkeit der Schweiz zentrale Mehrwerte der schweizerischen Volkswirtschaft bleiben und die wirtschaftliche Zukunft der Schweiz gesichert werden kann. Der Ansatz, sich im Grundsatz an die Verordnung (EU) 2016/679 (DSGVO) zu orientieren, ist sicherlich im Kontext der globalen Wirtschaft (Austausch Schweiz-EU) ein wichtiger und grundlegender Gesichtspunkt.

II. Stellungnahme zu einzelnen Artikeln

Zu Art. 1: Grundsätze

Bei den Grundsätzen zur Datensicherheit wird ein Schwerpunkt auf eine allgemeine Formulierung gelegt, da die Einzelfälle stark voneinander abweichen können und sachverhalts-bezogene, flexible und umsetzbare Lösungen erforderlich sind. Dieser Ansatz ist im Grundsatz sicherlich korrekt, kann jedoch in der Praxis zu Unsicherheiten und Auslegungsproblematiken führen. Hier wird die Rechtsprechung weitere Grundsätze entwickeln müssen, um die Grundpfeiler für die einzelnen Bereiche zu setzen. Auch vorstellbar ist, dass einzelne oder mehrere affine Branchen zusammen diese Grundsätze für ihre Branche(n) eigens erarbeiten müssen, um eine Rechtssicherheit schaffen zu können, vor allem auch im Hinblick darauf, dass bei einem Verstoss gegen diese Grundsätze strafrechtliche Folgen gemäss Art. 61 Buchstabe c nDSG drohen. Der SFF sieht somit diese umfassende Delegation der weiteren Konkretisierung der Grundsätze an die Judikative kritisch und stellt die Frage, ob mit dieser doch weiten Delegation das Prinzip der Gewaltentrennung nicht verletzt wird, indem die Judikative damit gezwungen wird, in den Kompetenzbereich der Legislative bzw. Exekutive einzugreifen. Gemäss der Ansicht des SFF wäre eine markantere Formulierung der Grundsätze wünschenswert und zielführend.
Im erläuternden Bericht zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz wird zu diesem Artikel auf Seite 14 ausdrücklich als Beispiel erwähnt, dass die Anforderungen zur risikobasierten Datensicherheit in einem Spital in aller Regel erhöhte Anforderungen im Vergleich zur Bearbeitung von Kunden- oder Lieferantendaten in einer Bäckerei oder Metzgerei sind. Der SFF als Branchenverband der Fleischbranche nimmt dieses Beispiel gerne auf und verlässt sich auf den Aussagewerte dieses Statements bei der zukünftigen Umsetzung der VDSG.

Zu Art. 1 Abs. 1 Buchstabe d: Für die Angemessenheit der ergriffenen technischen oder organisatorischen Massnahmen wird das Kriterium der Implementierungskosten genannt. Dieses Kriterium bezieht sich jedoch im Grundsatz nur auf die Wahl der kostengünstigeren Variante der technischen oder organisatorischen Massnahmen; eine Befreiung von der Pflicht einer angemessenen Datensicherheit kann nicht mit einer übermässigen Kostenverursachung begründet werden. Dies ist im Grundsatz korrekt, denn Datensicherheit ist ein unverzichtbares Gut. Dennoch stellt sich die Frage, welche Auswirkungen diese Bestimmung auf kleine KMU oder Kleinst-KMU oder auch Startups hat, für welche diese Umsetzung unverhältnismässig hohe Kosten verursacht. Dieser Punkt müsste unter diesem Gesichtspunkt noch genauer geprüft und mit einem Feintuning (beispielsweise einem Kostendach zwischen dem (voraussichtlichen) Umsatz und den Implementierungskosten) feinjustiert werden.

Zu Art. 1 Abs. 2: Die Massnahmen sollen in angemessenen Abständen überprüft werden. Der Begriff der «angemessenen Abstände» steht nach Ansicht des SFF individuellen Interpretationen zu weit offen. Anstelle dieses Begriffs zu präferieren wäre beispielsweise der Begriff «periodische Abständen, welche basierend auf der konkreten Gefährdungslage der Persönlichkeitsrechte und Grundrecht der Betroffenen definiert werden». Der in der VDSG gewählte Begriff der «angemessenen Abstände» lässt nach Ansicht des SFF zu viel Ermessensspielraum. Im Sinne der Rechtssicherheit und einer vereinheitlichten Umsetzung der Überprüfung der ergriffenen Massnahmen wäre eine gezielter greifende Definition im vorgeschlagenen Rahmen sinnvoll und zielführend.

Zu Art. 3: Gemäss dem erläuternden Bericht zur Totalrevision der VDSG kann die Protokollierung eine Massnahme für die Erreichung der Schutzziele gemäss Art. 2 VDSG sein. Damit wird eine Überschneidung mit Art. 2 VDSG willentlich in Kauf genommen. Nach Ansicht des SFF kann jedoch die Protokollierung nicht als technische oder organisatorische Massnahme zur Erreichung der Schutzziele angesehen werden, da diese abschliessend in Art. 2 genannt werden. Die Protokollierung dient der Folgeabschätzung bei einer automatisierten Bearbeitung von Personendaten und ist daher die Folge davon, dass die ergriffenen technischen oder organisatorischen Massnahmen nicht ausreichend greifen. Gemäss Ansicht des SFF wird damit eine Vermischung zwischen ergriffener Massnahmen und deren ungenügender Wirkung erreicht, die nicht sachkonform ist. Die Protokollierung kann nicht als ergriffene Massnahme zur Erreichung der Schutzziele qualifiziert werden, sondern als Instrument, um die inskünftig zu ergreifenden technischen oder organisatorischen Massnahmen zu definieren. Eine klare Abgrenzung zwischen den beiden Artikeln ist daher nach Einschätzung des SFF zwingend.

Zu Art. 8 Abs. 1 lit. c: Bei der Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs wird auf das Kriterium der Achtung der Menschenrechte abgestellt. Nach Ansicht des SFF hat dieses Kriterium keinen Platz bei der Beurteilung, ob ein Staat (bzw. ein Gebiet oder ein spezifischer Sektor) oder ein internationales Organ einen angemessen Datenschutz gewährleistet. Der Schutz der Menschenrechte ist sicherlich, ohne Zweifel und grundsätzlich ein wichtiger Aspekt, der bei

der Beantwortung verschiedener Fragen grundlegend ist. Bei der Evaluierung des Datenschutzes hat er jedoch keine Sachrelevanz und ist daher aus der Liste der Entscheidungskriterien zu streichen. Der SFF weist zudem darauf hin, dass die Prüfung der Achtung der Menschenrechte allenfalls schwierig sein und nur mit dem Einsatz erheblicher zeitlicher und finanzieller Mitteln gewährleistet werden kann. Ob die Evaluation abschliessend und sachgerecht abgeschlossen werden kann, bleibt zudem fraglich. Da eine solche Prüfung zudem nicht Datenschutz-relevant ist, macht der SFF beliebt, dieses Kriterium aus dem Evaluationskatalog ersatzlos zu streichen. Der SFF versteht nicht, warum die Schweiz sich in diesem Bereich in die Rolle des Hüters der Menschenrechte begibt und sich im Rahmen des Datenschutzes nicht nur darum bemüht, den Datenschutz optimal zu wahren und zu schützen.

Zu Art. 9 Abs. 3: Die Verantwortlichen und die Auftragsbearbeiter müssen die spezifischen Garantien des Datenschutzes nicht vom EDÖB genehmigen lassen, sondern ihm diese vor der Datenbekanntgabe ins Ausland bloss mitteilen. Damit wird ein nicht unbeträchtliches Risiko in Kauf genommen, dass die Risikobeurteilung durch die Verantwortlichen und Auftragsbearbeiter unterschiedlich erfolgt, dies sowohl im privaten wie auch im öffentlichen Sektor. Mit der nachtfolgenden, in Absatz 3 genannten Kriterien für den Mindestinhalt an solche spezifischen Garantien werden zwar gewisse einheitlichen Anforderungen gestellt, doch ist gemäss der Ansicht des SFF der Raum für individuelle und nur schlecht kalkulierbare Beurteilungsrisiken zu gross. Der SFF macht somit beliebt, diese blosse Informations- mit einer Genehmigungspflicht des EDÖB zu ersetzen.

Zu Art. 12 Abs. 2: Die Verhaltenskodizes und Zertifizierungen müssen vom EDÖB genehmigt werden, und dies, obwohl in diesem Artikel auf Art. 9 VDSG verwiesen wird, in welchem nur eine Informierung nicht eine Genehmigung des EDÖB vorgesehen wird. Der SFF kann den Grundsatz, wann der EDÖB nur informiert und wann er auch genehmigungspflichtig ist, nicht nachvollziehen, und macht, wie bereits vorstehend bei Art. 9 Abs. 3 erwähnt, eine Harmonisierung beliebt.

Zu Art. 16: Die Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten kann unterlassen werden, wenn damit ein unverhältnismässiger Aufwand verbunden ist. Weder die Verordnung noch der erläuternde Bericht zur Totalrevision der VDSG definieren diesen unverhältnismässigen Aufwand mit weiteren Details, so dass der Interpretationsspielraum im Einzelfall gemäss Ansicht des SFF zu weit ist und daher Raum dazu geschaffen wird, auf eine solche Information zu verzichten, um Aufwand zu vermeiden. Eine Definition mit Leitplanken, welche der Rechtssicherheit dienen, wäre gemäss dem SFF ins Auge zu fassen.

Zu Art. 26 Buchstabe a: Werden umfangreiche besonders schützenwerte Personendaten verarbeitet, gilt die Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten nicht. Dem SFF ist die Definition des Umfangs der verarbeiteten besonders schützenswerten Personendaten mit «umfangreich» juristisch zu unpräzise, da er zu grossen Interpretationsspielraum enthält. Der SFF bevorzugt eine engere Definition, beispielsweise eine, welche Bezug nimmt auf das Verhältnis aller Personendaten im Vergleich zu den besonders schützenswerten Personendaten.

Zu Art. 31: im Vergleich zum entsprechenden Text in der VDSG-Vorversion wird der Begriff der «unverzüglichen Information» durch den Begriff der «rechtzeitigen Information» ersetzt. Einmal mehr stellt der SFF fest, dass mit Neu- oder Umformulierungen Interpretationsraum geschaffen wird, der der Rechtssicherheit und einheitlichen Rechtsanwendung alles andere als förderlich ist. Denn hier ist nicht klar, was der Rechtsetzer unter dem Begriff der Rechtzeitigkeit konkret versteht. Neu ist es nun so, dass jedes Bundesorgan selber entscheidet, was unter einer rechtzeitigen Information an die Datenschutzberaterin/den Datenschutzberater zu verstehen ist. Die allfällig dadurch entstehenden Verzögerungen bei der Informationsübermittlung kann dann mit dem blossen Hinweis, dass der Zeitpunkt der Informierung als rechtzeitig erachtet wurde, legitimiert werden. Diese Legitimierung greift bei einer «unverzüglichen Information» nicht, weswegen der SFF beliebt man, den ursprünglichen Begriff wieder aufzunehmen.

Zu Art. 39 Abs. 2: Gemäss Ansicht des SFF wäre es sinnvoll, den Zeitpunkt des Einbezugs des EDÖB bei Rechtsetzungsentwürfen mit Bezug zur Bearbeitung von Personendaten, den Datenschutz sowie den Zugang zu amtlichen Dokumenten in der Verordnung selbst zu definieren, so wie dieser im erläuternden Bericht zur Totalrevision des VDSG auf Seite 46 erwähnt wird, nämlich mit dem Einbezug des EDÖB spätestens bei der Ämterkonsultation. Damit wird Klar- und Rechtsicherheit geschaffen und Auslegungsspielraum vermieden.

IV. Fazit

Der SFF unterstützt die Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz VDSG19-Verordnung Arbeitslosenversicherung unter Vorbehalt weniger Anmerkungen.

Wir danken Ihnen für die Berücksichtigung unserer Einschätzung.

Freundliche Grüsse

Schweizer Fleisch-Fachverband

Der Präsident

Dr. Ivo Bischofberger
alt Ständerat

Der Direktor

Dr. Ruedi Hadorn

SGB | USS
www.sgb.ch | www.uss.ch
Schweizerischer Gewerkschaftsbund
Union syndicale suisse
Unione sindacale svizzera

Eidg. Justiz- und Polizeidepartement EJPD

Elektronischer Versand an:
jonas.amstutz@bj.admin.ch

Bern, 14. Oktober 2021

Vernehmlassung zur Totalrevision der VDSG

Sehr geehrte Damen und Herren

Besten Dank für die Einladung zur oben erwähnten Vernehmlassung. Der SGB hat in der Vernehmlassung zur Totalrevision des Datenschutzgesetzes (nDSG) einen stärkeren Datenschutz für Arbeitnehmende gewünscht als vom Parlament schliesslich beschlossen. Vor diesem Hintergrund ist es für uns zentral, dass der Bundesrat in der Umsetzungsverordnung VDSG den vorhandenen Spielraum konsequent in Richtung hin zu mehr Datenschutz nutzt. Unter diesem Blickwinkel unterstützt der SGB den Inhalt der vorgeschlagenen Umsetzungsvorlage im Grundsatz, fordert allerdings in einigen Punkten klare Verbesserungen.

Kommentare zu den einzelnen Artikeln

Kriterien zur Beurteilung Angemessenheit der Datensicherheitsmassnahmen (Art. 1 Abs. 1 E-VDSG)

Für den SGB ist es zentral, dass die datenbearbeitenden Personen, insbesondere Arbeitgeber, ausreichende technische und organisatorische Massnahmen zur Gewährleistung der Sicherheit dieser Daten vornehmen. Vor diesem Hintergrund halten wir es für verfehlt, die Implementierungskosten als Beurteilungskriterium zur Angemessenheit solcher Massnahmen explizit in der Verordnung zu erwähnen.[1] So ist für uns z.B. das Risiko einer Verletzung der Datensicherheit das viel relevantere Beurteilungskriterium für die zu treffenden Massnahmen.

Folglich beantragt der SGB, Art. 1 Abs. 1 E-VDSG folgendermassen zu ändern:

Art. 1 Grundsätze

1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:

a. Zweck, Art, Umfang und Umstände der Datenbearbeitung;

b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen;

[1] Vgl. Erläuternder Bericht, S. 16.

Monbijoustrasse 61, 3007 Bern, www.sgb.ch
031 377 01 01, Fax 031 377 01 02, info@sgb.ch

c. der Stand der Technik;

~~**d. Implementierungskosten.**~~

2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.

Schutzziele zur Gewährleistung der Datensicherheit (Art. 2 E-VDSG)

Der SGB hält es für nicht angebracht, in der Umsetzungsverordnung explizit festzuschreiben, dass die Massnahmen zur Gewährleistung der Datensicherheit die Schutzziele nur insofern erreichen müssten, als diese Massnahmen angemessen seien.[2] Einerseits ist der Angemessenheitsgrundsatz bereits allgemein auf Gesetzesebene verankert (vgl. Art. 6 Abs. 5 nDSG), andererseits könnte die explizite Erwähnung der Angemessenheit den falschen Eindruck erwecken, die zur Sicherstellung der Datensicherheit zu erreichenden Schutzziele zu relativieren.

Folglich beantragt der SGB, Art. 2 E-VDSG folgendermassen zu ändern:

Art. 2 Schutzziele

~~**Soweit angemessen**~~, Die Massnahmen zur Gewährleistung der Datensicherheit müssen folgende Schutzziele erreichen:

Aufbewahrungsfrist der Protokolle bei automatisierter Datenbearbeitung mit hohem Risiko (Art. 3 Abs. 4 E-DSVG)

Für den SGB ist es wichtig, dass bei einer automatisierten Bearbeitung von Personendaten mit einem hohen Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen die entsprechenden Protokolle ausreichend lange aufbewahrt werden müssen, so dass allfällige Datenschutzverletzungen nachträglich nachvollzogen und daraus für zukünftige Datenbearbeitungen präventiv die richtigen Schlüsse gezogen werden können. Dies ist z.B. regelmässig der Fall bei automatisierten Einstellungsverfahren und der Führung von Personalakten. Vor diesem Hintergrund unterstützt der SGB die Verlängerung der Aufbewahrungsfrist dieser Protokolle gegenüber der geltenden Verordnung (vgl. Art. 10 Abs. 2) von 1 auf 2 Jahre.[3] Diese Frist darf folglich bei der Überarbeitung der Vorlage nicht gekürzt werden.

Vorgaben zur Bekanntgabe von Personendaten ins Ausland (Art. 8-12 E-VDSG)

Ganz allgemein ist es für den SGB wichtig, dass bei der Bekanntgabe von Personendaten ins Ausland der Bundesrat sicherstellt, dass der Datenschutz dabei ausreichend gewährleistet wird. Besonders Angestellte von Banken, etc., haben ein grosses Risiko, hier sonst ihre Daten in nicht äquivalente Rechts-Systeme transferiert zu sehen.

Vor diesem Hintergrund halten wir die Vorgaben in der neuen VDSG zur Beurteilung eines angemessenen Datenschutzniveaus von Staaten, Gebieten oder Sektoren grundsätzlich als sachgerecht und griffig[4]. Wir fordern deshalb den Bundesrat dazu auf, bei den entsprechenden Beurteilungen diese Vorgaben konsequent anzuwenden.

[2] Siehe Erläuternder Bericht, S. 17.
[3] Siehe Erläuternder Bericht, S. 20.
[4] Vgl. Erläuternder Bericht, S. 25ff.

Mindestanforderungen an Datenschutzklauseln und Garantien bei Bekanntgabe von Personendaten in Staaten ohne Angemessenheitsbeschluss des Bundesrates (Art. 9 E-VDSG)

Der SGB unterstützt den im Entwurf von Art. 9 E-VDSG enthaltenen Vorschlag des Bundesrates, für Datenschutzklauseln und spezifische Garantien bei der Bekanntgabe von Personendaten in Staaten ohne Angemessenheitsbeschluss des Bundesrates gewisse Mindestanforderungen auf Verordnungsstufe festzuschreiben. Diese Vorgaben sind umso wichtiger, weil diese Klauseln resp. Garantien gemäss den gesetzlichen Vorgaben (vgl. Art. 16 Abs. 2 lit. b nDSG) vom EDÖB nicht genehmigt, sondern nur zur Kenntnis genommen werden müssen.[5] Diese Klauseln sind restriktiv auszulegen. Gerade im Arbeitsverhältnis gesammelte Daten müssen besonders streng geschützt werden. Es besteht sonst regelmässig die Gefahr, dass Arbeitgeber um ihre Geschäftstätigkeit zu schützen ungerechtfertigt Daten ihrer Arbeitnehmenden ins Ausland bekannt geben.

Genehmigungspflicht des EDÖB von Verhaltenskodizes zur Bekanntgabe von Personendaten ins Ausland (Art. 12 Abs. 2 E-VDSG)

Um bei der Bekanntgabe von Personendaten ins Ausland gestützt auf unternehmensinterne Verhaltenskodizes die Sicherstellung eines angemessenen Datenschutzes wirksam kontrollieren zu können, begrüsst der SGB die vorgesehene Genehmigungspflicht dieser Verhaltenskodizes durch den EDÖB.[6]

Benachteiligungsverbot bei Verlangen der Überprüfung einer automatisierten Einzelentscheidung durch eine natürliche Person (Art. 17 E-VDSG)

Für den SGB ist es wichtig, dass Diskriminierungen bei automatisierten Einzelentscheidungen bestmöglich verhindert werden. Deshalb begrüssen wir es ausdrücklich, dass der Bundesrat in der Umsetzungsverordnung festschreiben will, dass Personen, welche die Überprüfung einer automatisierten Einzelentscheidung durch eine natürliche Person verlangen, dadurch nicht benachteiligt werden dürfen.[7] Damit soll richtigerweise verhindert werden, dass betroffene Personen davor zurückschrecken, eine solche Überprüfung einzufordern. Dies ist gerade im Arbeitsverhältnis ein reales Risiko, wo immer mehr HR-Entscheidungen automatisiert stattfinden (Management/Hiring/Firing by Algorithms). Dieser Schutz vor Diskriminierung bleibt aber nur theoretisch, solange der Kündigungsschutz in der Schweiz für Arbeitnehmende ungenügend ist, wie dies heute mit Art. 336a OR der Fall ist. Der SGB fordert deshalb, dass bei missbräuchlicher Kündigung wegen Ausübung des vorliegenden Rechts eine Erhöhung der zu zahlenden Entschädigung auf mindestens 24 Monatslöhne sowie die Wiedereinstellung stattfinden muss (parallele Revision von Art. 336a OR).

Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten bei KMU mit nicht umfangreicher Bearbeitung von besonders schützenswerten Personendaten (Art. 26 lit. a E-VDSG)

Um die Sicherstellung des Datenschutzes bei der Bearbeitung von besonders schützenswerten Personendaten auch bei KMUs zu gewährleisten, fordert der SGB, dass der Verzicht auf die Füh-

[5] Vgl. Erläuternder Bericht, S. 27.
[6] Siehe Erläuternder Bericht, S. 29.
[7] Siehe Erläuternder Bericht, S. 31.

rung eines Verzeichnisses der Bearbeitungstätigkeiten bei nicht umfangreicher Datenbearbeitung im Sinne von Art. 26 lit. a konsequent angewandt wird und dabei insbesondere der Begriff der umfangreichen Bearbeitung solcher Daten nicht zu restriktiv ausgelegt wird.[8]

Aus diesem Grunde ist auch KMUs die Führung eines Verzeichnisses betr. ihrer Mitarbeitenden vorzuschreiben.

Für die Berücksichtigung unserer Stellungnahme danken wir Ihnen im Voraus herzlich.

Freundliche Grüsse

SCHWEIZERISCHER GEWERKSCHAFTSBUND

Pierre-Yves Maillard
Präsident

Luca Cirigliano
Zentralsekretär

[8] Vgl. Erläuternder Bericht, S. 39f.

Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Bundesamt für Justiz
Herr
Jonas Amstutz
Bundesrain 20
3003 Bern

jonas.amstutz@bj.admin.ch

Bern, 11. Oktober 2021 sgv-Kl/ds

Vernehmlassungsantwort: Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

Als grösste Dachorganisation der Schweizer Wirtschaft vertritt der Schweizerische Gewerbeverband sgv über 230 Verbände und gegen 500 000 KMU, was einem Anteil von 99.8 Prozent aller Unternehmen in unserem Land entspricht. Im Interesse der Schweizer KMU setzt sich der grösste Dachverband der Schweizer Wirtschaft für optimale wirtschaftliche und politische Rahmenbedingungen sowie für ein unternehmensfreundliches Umfeld ein.

Mit Schreiben vom 23. Juni 2021 lädt das Eidgenössische Justiz- und Polizeidepartement EJPD ein, sich zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) zu äussern. Wir danken für die Einladung.

Die Verordnung zum Bundesgesetz über den Datenschutz enthält diverse Ausführungsbestimmungen, Anpassungen zum Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), einen Negativkatalog, welcher die risikobehafteten Datenbearbeitungen für die Führung eines Verzeichnisses der Bearbeitungstätigkeiten beinhaltet und weitere Bestimmungen, wie z. B. an die Datensicherheit.

Der Schweizerische Gewerbeverband sgv lehnt die vorliegende Version ab und begründet das wie folgt:

Generell

Der sgv stellt fest, dass das am 25. September 2020 verabschiedete Datenschutzgesetz durch eine engmaschige Verordnung ergänzt werden soll, wofür es in wesentlichen Punkten keine Gesetzesgrundlage gibt. Beispiele dafür sind die Protokollierungspflicht, das Bearbeitungsreglement, die Informationspflicht sowie Aufbewahrungs- und Dokumentationspflichten. Auch gehen diese Bestimmungen z. T. weiter als in der europäischen Datenschutzgrundverordnung. Der sgv lehnt diesen Swissfinish ab.

Zu einzelnen Artikeln

Art. 1 Grundsätze

Absatz 1: In Art. 1 Bst. d werden die «Implementierungskosten» als Angemessenheitskriterium für die Datensicherheit genannt. Allerdings werden damit nur die geldwerten Umsetzungsaufwendungen adressiert, nicht aber der Arbeitsaufwand der Verantwortlichen. Gerade in KMU kann dies eine erhebliche Belastung bedeuten, weshalb wir beantragen, statt «Implementierungskosten» den Begriff «**Implementierungsaufwand**» zu verwenden. Der Implementierungsaufwand umfasst den gesamten Aufwand des Verantwortlichen.

Absatz 2: *Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen* **ist ersatzlos zu streichen**. Eine permanente Überprüfung kann zu aufwendig werden und macht nur dann Sinn, wenn es wirklich zu relevanten Veränderungen eines Risikos kommt. Dannzumal soll eine Überprüfung wieder vorgenommen werden.

Art. 2 Schutzziele

Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen. Diese Bestimmung ist wie folgt umzuformulieren: «**Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele anstreben**:» Da es keine absolute Datensicherheit gibt (vgl. Swisscom), sollen Schutzziele angestrebt werden müssen.

Art. 2 legt zudem viele Schutzziele fest, die nicht in der alleinigen Verantwortung des Verantwortlichen liegen können. Zum Beispiel kann die Transportkontrolle durch viele externe Faktoren gefährdet werden, für welche der Verantwortliche gar nicht einstehen kann. Die Aufzählung von Art. 2 Bst. a bis k zeigt, dass die Last der «Privacy by design» vollumfänglich auf den Verantwortlichen im Betrieb abgewälzt wird, was der sgv nicht akzeptieren kann. **Die Aufzählung in Art. 2 Bst. a bis k ist in Beachtung dieser Problematik zu überarbeiten**. Dem Verantwortlichen dürfen nur Schutzziele auferlegt werden, die auch tatsächlich in seiner Verantwortung liegen.

Art. 3 Protokollierung

Die Protokollierungspflicht ist ersatzlos zu streichen. Sie ist nicht Gegenstand des Gesetzes, weshalb ihr die Rechtsgrundlage fehlt. Die dennoch in den Verordnungsentwurf aufgenommene Pflicht steht in keinem Verhältnis zum Nutzen. Protokolle sollen zwei Jahre lang aufbewahrt werden. Das beurteilt der Schweizerische Gewerbeverband sgv als unangemessen.

Art. 4 Bearbeitungsreglement von privaten Personen

Die Anforderungen mit der Konsequenz, dass viele Mikro- und Einpersonenbetriebe (z. B. Treuhänderinnen und Treuhänder) zuerst ein Berarbeitungsreglement verfassen müssten, bis sie es dann anwenden könnten. Zudem ist die Grundlage zur Pflicht betreffend Erstellung eines Reglements im Datenschutzgesetz nicht ersichtlich. Auch die «regelmässige Aktualisierung» gemäss Absatz 3 Art. 4 E-VDSG ist eine unverhältnismässige zusätzliche Belastung, die der sgv ablehnt. Art. 4 ist ersatzlos zu streichen.

Art. 6 Modalitäten

Absätze 1 und 2: Die Pflicht, für den Verantwortlichen, die vertrags- und gesetzesmässige Bearbeitung durch den Auftragsbearbeiter «sicherzustellen» ist im Ansatz falsch. Richtig ist, dass sich der Verantwortliche gemäss Art. 9 Abs. 2 DSG vergewissern muss, dass die Datenbearbeitung korrekt erfolgt (korrekt in Art. 6 Abs. 2, 1. Satz E-VDSG). Diese unverhältnismässige Verschärfung der Pflicht des Verantwortlichen hat nach Auffassung des sgv keine Rechtsgrundlage im DSG.

Formulierungsvorschlag für Art. 6 Abs. 1, 2. Satz E-VDSG: *Er vergewissert sich, dass die Daten vertrags- und gesetzesgemäss bearbeitet werden.*

Absatz 2 ist ersatzlos zu streichen. Von einer nicht dem DSG unterstellten Instanz kann nicht verlangt werden, dass sie Kenntnis der potentiell relevanten Gesetzesbestimmungen haben. Eventualiter ist folgender Formulierungsvorschlag für Art. 6 Abs. 2, 2. Satz E-VDSG vorzusehen: *Andernfalls muss er sich auf dem vertraglichen Weg vergewissern, dass ein gleichwertiger Datenschutz gewährleistet wird.*

Art. 8 Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs

Art. 8 adressiert sich an den Bund, wie das in den Erläuterungen (Seite 26) aufgeführt wird. Dies wird aber aus dem Verordnungsentwurf nicht klar. Aus diesem Grund ist Art. 8 E-VDSG zu ergänzen um: *«… einen angemessenen Schutz gewährleisten,* ***hat der Bundesrat namentlich folgende Kriterien zu berücksichtigen****…»*

Art. 9 Datenschutzklauseln und spezifische Garantien und

Art. 10 Standarddatenschutzklauseln

In Art. 9 Abs. 2 ist «sicherstellen» durch «sich vergewissern» zu ersetzen, ansonsten die Handhabbarkeit durch den Verantwortlichen kaum gegeben ist. Das Gleiche gilt für Art. 10 Abs. 1. Insbesondere die in Art. 9 E-VDSG gestellten Anforderungen erreichen ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Art. 9 Bst. h *(Massnahmen zur Gewährleistung der Datensicherheit)* ist ersatzlos zu streichen. Die übrigen Bestimmungen genügen, um einen angemessenen Schutz der Lieferung von Daten ins Ausland zu gewährleisten.

Art. 12 Verhaltenskodizes und Zertifizierungen

Artikel 12 ist zu ergänzen um einen Absatz 4: *Die Absätze 2 und 3 sind nicht anwendbar, wenn der EDÖB den Verhaltenskodex oder die Zertifizierung genehmigt hat*.

Art. 13 Modalitäten der Informationspflichten

Art. 19 DSG hält fest, dass der Verantwortliche die betroffene Person «angemessen» über die Beschaffung von Personendaten informiert, wobei diese Informationspflicht auch dann gilt, wenn die Daten nicht bei der betroffenen Person beschafft werden. Die Erläuterungen zur E-VDSG legen hingegen fest, dass die «wichtigsten Informationen» auf der «ersten Kommunikationsstufe» erfolgen müssen. Aus dem Gesetzeswortlaut folgt, dass die Mitteilung von den jeweiligen Umständen abhängig ist, was mit dem Begriff «angemessen» umschrieben wird. Dies ist entsprechend in den Erläuterungen festzuhalten. Art. 13 E-VDSG darf die im Gesetz verankerte «Angemessenheit» nicht aushöhlen.

Art. 15 Information bei der Bekanntgabe von Personendaten und

Art. 16 Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten

Es ist nicht ersichtlich, welches die gesetzliche Grundlage für diese Informationspflichten sein soll. Beide Artikel sind deshalb ersatzlos zu streichen.

Art. 18 Form und Aufbewahrung der Datenschutz-Folgenabschätzung

Auch in Bezug auf die zweijährige Aufbewahrungsfrist nach Beendigung der Datenbearbeitung ist die gesetzliche Grundlage unklar. Der Passus «*Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden*.» ist ersatzlos zu streichen.

Art. 19 Meldung von Verletzungen der Datensicherheit

Art. 24 DSG regelt die Meldung von Verletzungen der Datensicherheit. Art. 19 Abs. 1 Bst. b bis d E-VDSG geht gegenüber der Gesetzesgrundlage viel zu weit. Die betreffenden Buchstaben sind ersatzlos aus der Verordnung zu streichen, da für diese detaillierte Aufzählung die gesetzliche Grundlage fehlt.

Gemäss Art. 19 Abs. 1 Bst. e meldet der Verantwortliche dem EDÖB «die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen». Aus Natur der Sache wird es gar nicht immer möglich sein, die Folgen zu melden. Bestenfalls können Folgen «soweit möglich» oder Folgen «soweit vermutet» angenommen werden. Die Verordnung ist in diesem Sinne anzupassen.

Die Dokumentations- und Aufbewahrungspflicht gemäss Art. 19 Abs. 5 E-VDSG geht sehr weit. Nach Auffassung des sgv fehlt es an einer gesetzlichen Grundlage dafür.

Art. 20 Modalitäten des Auskunftsrechts

Art. 20 E-VDSG umschreibt die Modalitäten des Auskunftsrechts sehr engmaschig. Auch hier ist die gesetzliche Grundlage fraglich. Das gilt insbesondere für Abs. 5, der festlegt, dass «der Verantwortliche die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft «zu dokumentieren hat und die Dokumentation mindestens drei Jahre lang aufzubewahren hat». Konsequenterweise ist Abs. 5 ersatzlos zu streichen. Abs. 3 ist zu ergänzen um «*… verständlich sein, soweit dies im Rahmen des kognitiven Zustands möglich ist.»*

Art. 22 Frist

Der Fristenbeginn ist zu präzisieren. Er kann nur dann beginnen, wenn das Auskunftsgesuch formell korrekt eingereicht und inhaltlich klar ist. Solange das Gesuch entweder formell oder inhaltlich unklar ist, kann die Frist nicht laufen.

Art. 23 Ausnahmen von der Kostenlosigkeit

Bei Aufwendungen, die weit über CHF 1'000.00 gehen können, ist eine Kostenbeteiligung von nur gerade CHF 300.00 nicht angemessen. Der Verantwortliche hat die Kosten zu belegen. Es darf aber nicht sein, dass der Verantwortliche auf einem Kostenberg sitzen bleibt und vom Kostenverursacher nur ein symbolischer Betrag einverlangt werden kann. Der Höchstbetrag ist deshalb anzuheben und sollte auf mindestens CHF 1'000.00 festgelegt werden.

Art. 24 Datenportabilität

Da die Datenportabilität erst im Verlaufe der Beratungen ins DSG aufgenommen worden ist, fehlt es an präzisierenden Angaben. Der Anspruch auf Datenportabilität bei der Datenherausgabe oder -übertragung darf nicht ein absoluter sein. Dieser Anspruch darf nur bestehen, soweit die Bearbeitung von Personendaten in gängigen Formaten erfolgen kann bzw. erfolgt. Deshalb fordert der sgv eine Ergänzung in dem Sinne, dass «*das Recht der betroffenen Person, die betreffenden Personendaten vom Verantwortlichen heraus zu verlangen oder durch diesen an einen anderen Verantwortlichen übertragen zu lassen, für die Verantwortlichen nicht die Pflicht, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten, begründet.*

Art. 26 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: Es werden umfangreich besonders schützenswerte Personendaten bearbeitet oder es wird ein Profiling mit hohem Risiko durchgeführt. Diesbezüglich ist zu präzisieren, dass sich die allfäl-

lige Pflicht eines KMU (unter den beiden genannten Voraussetzungen) nicht auf sämtliche Bearbeitungen erstreckt, sondern nur auf diejenigen, die in den Voraussetzungen explizite erwähnt sind. Ausserdem ist zu präzisieren, dass das Verzeichnis nicht schriftlich, sondern auch in anderer Form, z. B. elektronisch geführt werden kann. Sodann braucht es eine klare Abgrenzung für die Ausnahmefälle: Was heisst «umfangreich besonders schützenswerte Personendaten»? Wenn keine (messbaren) Präzisierungen gemacht werden, könnte das zu grossen Rechtsunsicherheiten führen.

Art. 45 Gebühren

Wenn die Kostenbeteiligung nach Art. 23 mit den Gebührengrundsätzen des EDÖB verglichen wird, fällt eine krasse Diskrepanz auf. Der EDÖB erledigt eine Tätigkeit im Interesse der Gesellschaft und Öffentlichkeit. Es gibt keinen nachvollziehbaren Grund, weshalb die Person, welche Dienstleistungen von ihm braucht, um sich datenschutzkonform zu verhalten, derart zur Kasse gebeten wird. Weder kann es sein, dass die Gebühren nach Zeitaufwand berechnet werden (die Privatperson hat keinen Einfluss auf die Effizienz der Leistungserbringung durch den EDÖB), noch sind die Stundensätze von CHF 150.00 bis 350.00 in irgendeiner Weise angemessen. Die Gebührenordnung ist aus diesem Grund vollständig zu überdenken und nach einem vernünftigen Mass anzupassen.

Inkraftsetzung und Übergangsbestimmungen

Die Totalrevision des Datenschutzrechtsrechts bringt weitgehende Änderungen und hat neue Verpflichtungen für die Unternehmen zur Folge. Eine angemessene Umsetzungsfrist ist deshalb notwendig, zumal im neuen DSG keine Übergangsfristen vorgesehen sind und das neue Recht (totalrevidiertes DSG samt totalrevidiertem Verordnungsrecht) bei dessen Inkrafttreten bereits vollständig implementiert sein sollte. Dies sollte bei der Festlegung des Inkraftsetzungstermins berücksichtigt werden. Für die Umsetzungsarbeiten in den Unternehmen erachten wir einen Zeitraum von mindestens einem Jahr, laufend ab Feststehen/Veröffentlichung der definitiven Fassung der Verordnung, als notwendig.

Wir danken für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Schweizerischer Gewerbeverband sgv

Hans-Ulrich Bigler
Direktor

Dieter Kläy
Ressortleiter

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

Frau Bundesrätin Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Börsenstrasse 15
Postfach, CH-8022 Zürich
Telefon +41 58 631 00 00
Fax +41 58 631 50 00
www.snb.ch

Zürich, 21. Oktober 2021

Recht
recht@snb.ch
OERT-1278050686-84708

Vernehmlassung zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz

Stellungnahme

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Der Bundesrat hat im Juni 2021 die Vernehmlassung zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (nachfolgend «E-VDSG») eröffnet und zur Stellungnahme bis zum 14. Oktober 2021 eingeladen. Für die Schweizerische Nationalbank (nachfolgend «SNB») wurde die Frist zur Stellungnahme freundlicherweise bis zum 22. Oktober 2021 verlängert.

Als unabhängige Zentralbank führt die SNB die Geld- und Währungspolitik der Schweizerischen Eidgenossenschaft. Zu ihren Aufgaben gehört die Versorgung des Schweizerfranken Geldmarkts mit Liquidität, die Gewährleistung der Bargeldversorgung, die Erleichterung des Funktionierens der bargeldlosen Zahlungssysteme, die Verwaltung der Währungsreserven und die Leistung eines Beitrags zur Stabilität des Finanzsystems. Ferner wirkt die SNB bei der internationalen Währungskooperation mit und erbringt dem Bund Bankdienstleistungen. Im Zuge ihrer Aufgabenerfüllung bearbeitet die SNB auch Personendaten. Entsprechend werden das totalrevidierte Datenschutzgesetz und die einschlägige Verordnung die Datenbearbeitungen durch die SNB beeinflussen.

Vor diesem Hintergrund nimmt die SNB die Gelegenheit zur Stellungnahme zum E-VDSG gerne wahr. Die SNB unterstützt die allgemeine Stossrichtung des neuen Datenschutzgesetzes, insbesondere die damit verbundene Angleichung an das europäische Recht ist aus unserer Sicht hilfreich. Allerdings scheint uns, dass bei mehreren Bestimmungen der E-VDSG die gesetzliche Grundlage im revDSG zumindest fraglich ist. Auch führen einzelne Bestimmungen zu Doppelspurigkeiten und aus unserer Sicht unnötigem Mehraufwand. Schliesslich scheinen Begriffsklärungen und Präzisierungen empfehlenswert.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme. Sollten weitere Erläuterungen seitens der SNB erforderlich sein, stehen wir gerne zur Verfügung.

Freundliche Grüsse
Schweizerische Nationalbank

Peter Schöpf
Generalsekretär

Dr. Martin Plenio
Leiter Recht

Beilage: Stellungnahme der Schweizerischen Nationalbank zum E-VDSG

Stellungnahme der SNB zum E-VDSG

Alle Artikelangaben beziehen sich ohne andere Angabe auf den E-VDSG.

Zu Art. 2 – Schutzziele

Antrag: Art. 2 sollte dahingehend präzisiert werden, dass ein Hinwirken auf die Schutzziele ausreichend ist.

Begründung: Die Schutzziele in Art. 2 sind als (allgemeine) Ziele zu verstehen (vgl. Art. 8 revDSG). Die vorgeschlagene Formulierung suggeriert aber, dass sie in jedem Zeitpunkt der Datenbearbeitung erfüllt sein müssen. Einmal abgesehen davon, dass in vielen Fällen nicht jedes Schutzziel relevant ist, ist eine absolute Sicherheit im Sinne eines Nullrisikos nicht möglich (siehe Art. 8 Abs. 1 revDSG, welcher nur eine «angemessene» Datensicherheit verlangt).

Zu Art. 3 Abs. 1 – Protokollierung

Antrag: Art. 3 Abs. 1 sollte gestrichen werden.

Begründung: Art. 3 Abs. 1 soll Art. 8 Abs. 3 revDSG ausführen, allerdings betrifft Art. 8 Abs. 3 revDSG nur die Datensicherheit im eigentlichen Sinn (nur ihre Verletzung kann strafrechtliche Konsequenzen haben), nicht die Verletzung einer Protokollierungspflicht (vgl. Art. 61 lit. c revDSG). Im Zuge der parlamentarischen Arbeiten zur Datenschutz-Folgenabschätzung in Art. 22 revDSG wurde keine Protokollierungspflicht im Sinne von Art. 3 Abs. 1 ins Gesetz aufgenommen. Die in Art. 3 Abs. 1 angesprochene Datenschutz-Folgenabschätzung bewertet ein Risiko, sie eignet sich aber nicht zur Feststellung, ob die Datensicherheit verletzt ist, und entsprechend auch nicht zur Begründung einer Protokollierungspflicht unter diesem Titel. Schliesslich sieht Art. 23 revDSG vor, dass die Stellungnahme des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (nachfolgend «**EDÖB**») eingeholt werden muss, wenn die Datenschutz-Folgenabschätzung ergibt, dass – trotz vorgesehener Massnahmen – noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht. Auch vor diesem Hintergrund erweist sich eine weitergehende Protokollierungspflicht im Sinne von Art. 3 Abs. 1 als unverhältnismässig.

Zu Art. 3 Abs. 2 – Protokollierung

Antrag: Art. 3 Abs. 2 sollte gestrichen werden.

Begründung: Art. 3 Abs. 2 statuiert unabhängig vom Risiko für die betroffene Person eine Protokollierungspflicht für Bundesorgane bei einer automatisierten Bearbeitung von Personendaten. Dabei wird nicht definiert, was unter einer «automatisierten Bearbeitung» zu verstehen ist. Je nach Interpretation ist praktisch jede Bearbeitung eine automatisierte

Bearbeitung, was als allgemeine Protokollierungspflicht für jede Bearbeitung, unabhängig vom effektiven Risiko, interpretiert werden kann. Das ist aus unserer Sicht nicht verhältnismässig. Dies wird dadurch verschärft, dass die Protokollierungspflicht nach Art. 3 Abs. 2 auch den Vorgang des «Lesens» umfasst. Wie bereits zu Art. 3 Abs. 1 ausgeführt, fehlt der Bestimmung zudem eine gesetzliche Grundlage.

Zu Art. 3 Abs. 3 – Protokollierung

Antrag: Art. 3 Abs. 3 sollte gestrichen werden.

Begründung: Vgl. oben, Ausführungen zu Art. 3 Abs. 1. Zudem steht Abs. 3 im Widerspruch zu Art. 3 Abs. 1 und Abs. 2, da er über diese hinausgeht.

Zu Art. 3 Abs. 4 – Protokollierung

Antrag: Art. 3 Abs. 4 sollte gestrichen werden.

Begründung: Vgl. oben.

Zu Art. 4 – Bearbeitungsreglement von privaten Personen

Antrag: Art. 4 sollte gestrichen werden.

Begründung: Die Regelung von Art. 4 Abs. 1 wurde aus Art. 11 der geltenden VDSG übernommen. Allerdings scheint uns dafür eine gesetzliche Grundlage zu fehlen. Art. 8 Abs. 3 revDSG ist jedenfalls keine solche, da das Bearbeitungsreglement im Sinne von Art. 4 Abs. 1 die Einhaltung der Bearbeitungsgrundsätze sicherstellen möchte. Das revDSG sieht verschiedene Dokumentationspflichten vor (Verzeichnisse von Bearbeitungstätigkeiten [Art. 12 revDSG] und Datenschutz-Folgenabschätzungen [Art. 22 revDSG]). Diese Ordnung ist unseres Erachtens als abschliessend zu betrachten. Die genannten Dokumentationspflichten stellen bereits sicher, dass Bearbeitungstätigkeiten aufgezeichnet werden (Doppelspurigkeiten).

Zu Art. 5 – Bearbeitungsreglement von Bundesorganen

Antrag: Art. 5 sollte gestrichen werden.

Begründung: Die extensive Auflistung der Faktoren in Art. 5 Abs. 1 führt dazu, dass für jede automatisierte Bearbeitung von Personendaten ein Bearbeitungsreglement erstellt werden müsste. Mit Blick darauf, dass im revDSG bereits verschiedene Dokumentationspflichten verankert sind, wird sichergestellt, dass Bearbeitungstätigkeiten aufgezeichnet werden. Art. 5 Abs. 1 scheint daher unnötig. Auch fehlt dieser Bestimmung aus unserer Sicht eine gesetzliche Grundlage.

Zu Art. 6 Abs. 1 – Modalitäten

Antrag: Art. 6 Abs. 1 sollte gestrichen oder angepasst werden (bspw. «Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, trägt dafür Sorge, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden»).

Begründung: Art. 6 Abs. 1 suggeriert, dass eine – vom Gesetzgeber unseres Erachtens nicht vorgesehene – Kausalhaftung besteht. Für eine solche fehlt aber eine gesetzliche Grundlage.

Zu Art. 7 – Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans

Antrag: Art. 7 sollte gestrichen werden. Eventualiter ist in Art. 7 Satz 2 zu präzisieren, was mit «Problemen» gemeint ist.

Begründung: Art. 29 sieht bereits eine Informationspflicht von Bundesorganen an die Datenschutzberaterin bzw. den Datenschutzberater vor. Art. 7 ist daher redundant.

Zu Art. 9 Abs. 2 – Datenschutzklauseln und spezifische Garantien

Antrag: Die Formulierung «sicherstellen» sollte durch «Sorge zu tragen» ersetzt werden.

Begründung: Es ist nicht möglich, die Einhaltung eines Vertrags durch die Gegenpartei «sicherzustellen».

Zu Art. 13 Abs. 1 – Modalitäten der Informationspflichten

Antrag: Die Erwähnung des Auftragsbearbeiters ist aus unserer Sicht zu streichen. Zudem sollte «mitteilen» durch «informieren» ersetzt werden.

Begründung: Nach Art. 19 revDSG hat ausschliesslich der Verantwortliche eine Informationspflicht. Es fehlt an einer gesetzlichen Grundlage für eine Informationspflicht auch des Auftragsbearbeiters gemäss Art. 13 Abs. 1. Art. 19 revDSG sieht ferner vor, dass der Verantwortliche die betroffene Person «informiert» («mitteilen» könnte als Verschärfung interpretiert werden). Die Bestimmung könnte zudem dahingehend ergänzt werden, dass eine Information auf der Internetseite des Verantwortlichen grundsätzlich genügt.

Zu Art. 14 – Informationspflicht der Bundesorgane bei der systematischen Beschaffung von Personendaten

Antrag: Die Bestimmung sollte ergänzt werden mit dem Zusatz «soweit dies nicht aus den Umständen ersichtlich ist».

Begründung: Die Bestimmung berücksichtigt nicht, dass in vielen Fällen bereits aufgrund der Umstände offensichtlich ist, dass eine Auskunft freiwillig ist. Dies ist in Art. 14 zu berücksichtigen.

Zu Art. 18 – Form und Aufbewahrung der Datenschutz-Folgenabschätzung

Antrag: Art. 18 Satz 1 sollte so formuliert sein, dass die Datenschutz-Folgenabschätzung in jeder Form, die einen Nachweis mittels Text ermöglichen, festgehalten werden kann. Art. 18 Satz 2 kann gestrichen werden. Eventualiter ist Art. 18 Satz 2 so zu präzisieren, dass klar wird, dass es um die jeweils aktuellste Fassung der Datenschutz-Folgenabschätzung geht und dass die zweijährige Frist eine Mindestfrist darstellt.

Begründung: «Schriftlichkeit» im Sinne von Art. 18 Satz 1 kann nicht bedeuten, dass eine Datenschutz-Folgenabschätzung in Papierform ausgedruckt und unterschrieben wird. Dafür würde eine gesetzliche Grundlage fehlen, und es gibt auch kein Bedürfnis dafür.

Unseres Erachtens besteht auch kein Grund für eine Aufbewahrungspflicht, da es im Interesse des Verantwortlichen liegt, die Durchführung der Datenschutz-Folgenabschätzungen nachweisen zu können. In jedem Fall sollte präzisiert werden, dass es sich bei der Aufbewahrungsfrist um eine Mindestfrist handelt. Da Datenschutz-Folgenabschätzungen periodisch erneuert werden können, sollte zudem nur die aktuellste Fassung der Datenschutz-Folgenabschätzung aufbewahrt werden müssen.

Zu Art. 19 Abs. 5 – Meldung von Verletzungen der Datensicherheit

Antrag: Art. 19 Abs. 5 sollte gestrichen werden.

Begründung: Im revDSG fehlt eine gesetzliche Grundlage für eine eigentliche Dokumentationspflicht im Sinne von Art. 19 Abs. 5. Der EDÖB kann bei Bedarf weitere Informationen einfordern. Eine eigenständige Dokumentationspflicht im Sinne von Art. 19 Abs. 5 ist daher nicht notwendig und kann gestrichen werden. Es ist im Übrigen nicht ersichtlich, weshalb eine dreijährige Aufbewahrungsfrist statuiert wird, wenn das revDSG und die E-VDSG ansonsten jeweils zweijährige Fristen vorsehen.

Zu Art. 20 Abs. 5 – Modalitäten

Antrag: Art. 20 Abs. 5 kann gestrichen werden.

Begründung: Das revDSG enthält unseres Erachtens keine gesetzliche Grundlage für eine Dokumentations- und Aufbewahrungspflicht im Sinne von Art. 20 Abs. 5. Die Bestimmung würde zudem dazu führen, dass die Verantwortlichen Personendaten länger aufzubewahren bzw. mehr Personendaten zu bearbeiten haben, als dies geplant ist. Der Zweck von Art. 20 Abs. 5 wird durch die schriftliche Antwort (Art. 20 Abs. 1) bereits erfüllt.

Zu Art. 29 Abs. 2 – Modalitäten

Antrag: Die Bestimmung ist dahingehend zu präzisieren, dass die Veröffentlichung einer E-Mail-Adresse zur Kontaktaufnahme genügt.

Begründung: Aus Gründen des Persönlichkeitsschutzes sollte der Name der Datenschutzberaterin oder des Datenschutzberaters nicht publiziert werden müssen.

Zu Art. 31 – Information an die Datenschutzberaterin oder den Datenschutzberater

Antrag: Die Formulierung «sogleich» in Art. 31 zweiter Teilsatz sollte durch «angemessen» ersetzt oder gestrichen werden.

Begründung: Eine «angemessene» Berücksichtigung der Erfordernisse des Datenschutzes scheint uns praktikabler.

Zu Art. 32 Abs. 1 – Meldung an den EDÖB

Antrag: Art. 32 Abs. 1 sollte gestrichen werden.

Begründung: Die Botschaft zu Art. 11 Abs. 4 E-DSG (nun Art. 12 Abs. 4 revDSG) führt aus, dass keine Änderungen zum bestehenden Recht vorgesehen seien (BBl 2017 6941 7037). Das geltende Datenschutzrecht verpflichtet Bundesbehörden nicht, dem EDÖB geplante Datensammlungen zu melden. Im revDSG wurde ebenfalls keine gesetzliche Grundlage für eine Meldepflicht für Datensammlungen an den EDÖB im Sinne von Art. 32 Abs. 1 geschaffen. Die Bestimmung sollte daher gestrichen werden.

Zudem ist die Verhältnismässigkeit von Art. 32 Abs. 1 höchst fraglich. Es müssten automatisierte Bearbeitungstätigkeiten gemeldet werden, die lediglich geplant sind. Unklar bliebe, ab wann eine Bearbeitung «geplant» ist. Für Bundesbehörden führt dies zudem zu erheblichem Mehraufwand – besonders, weil nicht nur geplante automatisierte Bearbeitungstätigkeiten mit erhöhtem Risiko zu melden sind, sondern alle geplanten automatisierten Bearbeitungstätigkeiten. Schliesslich müsste die Meldung im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung erfolgen; in diesem Zeitpunkt liegen die notwendigen Informationen jedoch oft noch nicht in einem Detaillierungsgrad vor, der eine Meldepflicht rechtfertigen würde.

* * * * *

Geschäftsstelle
Swiss Payment Association
Ohmstrasse 11
8050 Zürich
www.swiss-payment-association.ch

Kontakt
Telefon: +41 58 426 25 55
office@swiss-p-a.ch

Swiss Payment Association, Ohmstrasse 11, 8050 Zürich

Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
3003 Bern
PER MAIL: jonas.amstutz@bj.admin.ch

Zürich, 11. Oktober 2021

Stellungnahme der Swiss Payment Association (SPA) zur Revision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrter Herr Amstutz

Wir bedanken uns für die Möglichkeit, uns zum Entwurf der totalrevidierten Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) vernehmen zu lassen. Gerne lassen wir Ihnen hiermit unsere Stellungnahme zukommen.

Vorab gestatten wir uns den Hinweis, dass der Swiss Payment Association (SPA) alle grossen Schweizer Herausgeber[1]von Kreditkarten der internationalen Kartenorganisationen mit gegen 8 Millionen herausgegebenen Karten angehören. Als Branchenorganisation vertritt die SPA die Positionen ihrer Mitglieder im Dialog mit all deren Anspruchsgruppen.

1. Kapitel: Allgemeine Bestimmungen

Das neue Datenschutzgesetz (nDSG) verfolgt einen risikobasierten Ansatz. Auf dieser Grundlage ist der Bundesrat nach Art. 8 Abs. 3 nDSG aufgefordert, Bestimmungen über die Mindestanforderungen an die Datensicherheit zu erlassen. Im 1. Kapitel (Allgemeine Bestimmungen), 1. Abschnitt (Datensicherheit), der E-VDSG finden sich nach Auffassung der SPA jedoch keine derartigen Mindestanforderungen.

[1] Mitglieder der Swiss Payment Association sind die Schweizer Kreditkarten-Herausgeber Cembra Money Bank AG, Cornèr Bank AG, PostFinance AG, Swisscard AECS GmbH, UBS Switzerland AG und Viseca Payment Services SA.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
1	1	a	Ziel der Bestimmung ist es, Kriterien zu nennen, anhand derselben beurteilt werden kann, ob die technischen/organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessen sind, das von der Datenbearbeitung ausgeht. Unseres Erachtens wird über die meisten der aufgeführten Kriterien jedoch kein Bezug zum Risiko hergestellt, das von einer bestimmten Datenbearbeitung ausgeht.	Es sind Kriterien zu benennen, über die ein Bezug zum Risiko hergestellt werden kann, das von einer konkreten Datenbearbeitung ausgeht (basierend auf Art. 8 Abs. 1 nDSG).
1	1	d	Einerseits ist das Kriterium «Implementierungskosten» unpräzise und damit wenig tauglich. Andererseits erscheint das Kriterium «Implementierungskosten» mit Blick auf die Ausführungen im Erläuternden Bericht als zweitklassig, da es im Bericht stark relativiert wird (es soll nur herangezogen werden dürfen, um zwischen gleichwertigen Massnahmen zur Gewährleistung der Datensicherheit die kostengünstigste wählen zu können). Die vorgenommene Relativierung ist willkürlich und nicht nachvollziehbar.	Anstelle von «Implementierungskosten» sollte der Begriff «Implementierungsaufwand» verwendet werden. Kosten hängen stark von der individuellen Betriebsorganisation ab und fallen dementsprechend für den gleichen Sachverhalt von Betrieb zu Betrieb unterschiedlich aus. Das Kriterium «Kosten» ist daher ungeeignet. Unter den Begriff «Implementierungsaufwand» fallen demgegenüber sämtliche Implementierungs-Aufwendungen bzw. sämtliche für die Implementierung massgeblichen Kostenträger, wie z.B. auch personelle, zeitliche und organisatorische. Es ist klarzustellen, dass die relativierenden Ausführungen im Erläuternden Bericht unzutreffend sind. Denn wenn in Art. 1 Abs. 1 lit. a-d Kriterien zur Beurteilung der Angemessenheit der Massnahmen aufgelistet werden und sich darunter auch das Kriterium der Implementierungskosten befindet, kann dieses den anderen Kriterien nicht nachstehen.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
1	2		Die Verpflichtung, die Massnahmen "in angemessenen Abständen" zu überprüfen, führt zu weit. Wenn sich an einer konkreten Datenbearbeitung nichts Wesentliches geändert hat und somit keine neuen Risikofaktoren hinzugekommen sind, ist eine periodische Überprüfung unverhältnismässig. Zudem fehlt es dieser auf Verordnungsstufe eingefügten Verpflichtung an der gesetzlichen Grundlage.	Auf die Pflicht, zur Überprüfung der Massnahmen ist zu verzichten Eventualiter soll die Überprüfung nicht in «angemessenen Abständen», sondern «in angemessener Weise» erfolgen.
2			Es wird verlangt, dass die Massnahmen zur Gewährleistung der Datensicherheit bestimmte Schutzziele «erreichen». Es ist nicht möglich, dass jemand (z.B. der Verantwortliche) garantieren kann, dass bestimmte Ziele erreicht werden. Art. 8 Abs. 2 nDSG verlangt nicht, dass bestimmte Schutzziele zu erreichen sind, sondern dass Verletzungen der Datensicherheit zu vermeiden sind. Einzelne angeführte Schutzziele verlangen Unmögliches bzw. sind überschiessend, zu detailliert oder zu absolut. Gemäss lit. b muss der Zugang «unbefugten Personen verwehrt» werden. Lit. c verlangt, dass unbefugten Personen der Zugriff auf Datenträger «verunmöglicht» wird. Weiter ist in lit. d und in lit. e von «verhindern» die Rede. Und in lit. j wird «gewährleisten» verlangt. Um Praxistauglichkeit zu erreichen, ist eine Reduktion auf das Wesentliche erforderlich. Zu den Schutzzielen wird im Erläuternden Bericht (S. 17) ausgeführt: «Ist ein Schutzziel in einem Fall nicht von Relevanz, so müssen der Verantwortliche und Auftragsbearbeiter aber in der Lage sein, zu begründen, weshalb dies der Fall ist.» Diese Begründungspflicht bei Nicht-Berücksichtigung führt zu einem grossen administrativen Aufwand.	Anstatt Schutzziele zu erreichen, müssen die Massnahmen ermöglichen, Verletzungen der Datensicherheit zu vermeiden. Die Verordnungsbestimmung ist konsequent auf diese gesetzliche Vorgabe auszurichten. Entsprechend den Ausführungen im erläuternden Bericht sollten die Massnahme auf die aufgelisteten Schutzziele «ausgerichtet werden.» Art. 2 Satz 1 könnte wie folgt formuliert werden: «Die Massnahmen zur angemessenen Vermeidung von Verletzungen der Datensicherheit sind, soweit von Relevanz, auf folgende Schutzziele auszurichten:». Der überschiessende Katalog der Schutzziele soll durch die klassischen Schutzziele «Vertraulichkeit», «Integrität» und «Verfügbarkeit» ersetzt werden. Es soll nicht jedes Mal bzw. für jedes nicht verfolgte Schutzziel begründet werden müssen, warum keine Berücksichtigung des Schutzziels stattfinden kann. Vielmehr soll anhand der Datenbearbeitung eruiert werden, welche Schutzziele vernünftigerweise in Frage kommen. Das Resultat dieses Prozesses ist mit kurzer Begründung zu dokumentieren.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
3			Für die in Art. 3 statuierte Protokollierungspflicht gibt es im nDSG keine gesetzliche Grundlage. Ebenso gibt es keine gesetzliche Grundlage für die Aufbewahrungspflicht von zwei Jahren.	Die Protokollierungspflicht ist aus der E-VSDG zu streichen. Im Minimum ist klarzustellen, dass es sich bei der Protokollierung um keine Mindestanforderung an die Datensicherheit handelt. Zudem ist auf die Regelung der Aufbewahrungsdauer, auf die enge Zweckbindung und auf die strenge Zugangsbeschränkung zu verzichten.
4	1 und 2		Für die in Art. 4 Abs. 1 E-VDSG statuierte Pflicht zur Erstellung eines Bearbeitungsreglements gibt es im nDSG keine gesetzliche Grundlage. Weiter ist der Zweck des Bearbeitungsreglements nicht ersichtlich, da private Verantwortliche bereits ein Bearbeitungsverzeichnis führen (siehe Art. 12 nDSG), das teilweise deckungsgleich mit dem vorgesehenen Bearbeitungsreglement ist. Zudem decken bereits die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung sowie die zwingende Offenlegung von automatischen Bearbeitungen, die besonders schützenswerte Personendaten betreffen, alle Anforderungen ab, welche über das Reglement erfüllt werden sollen.	Art. 4 E-VDSG ist ersatzlos zu streichen.
4	3		Art. 4 Abs. 3 statuiert, dass der Verantwortliche das Bearbeitungsreglement der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zu Verfügung stellt. Dazu ist festzuhalten, dass sich aus dem nDSG keine Pflicht zur Ernennung einer Datenschutzberaterin/eines Datenschutzberaters ergibt, womit auch keine Verpflichtung bestehen kann, die Beraterin oder den Berater mit einem Reglement zu versehen. Zudem ist nicht klar, was mit «in verständlicher Form» gemeint ist.	Art. 4 E-VDSG ist ersatzlos zu streichen.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
6	1		Art. 6 Abs. 1 verlangt, dass der Verantwortliche «sicherstellt», dass ein Auftragsbearbeiter die Daten vertrags- oder gesetzesgemäss bearbeitet. Diese absolute Formulierung führt zu weit und ist realitätsfern. Art. 9 nDSG statuiert eine datenschutzrechtliche Sorgfaltspflicht des Verantwortlichen, verlangt aber zu Recht kein «Sicherstellen», dass der Auftragsbearbeiter die Daten vertrags- oder gesetzesgemäss bearbeitet (denn das kann der Verantwortliche nicht sicherstellen bzw. nicht garantieren). Es fehlt damit an einer gesetzlichen Grundlage für die Pflicht zur Sicherstellung einer gesetzes- und vertragskonformen Datenbearbeitung. Der erste Satz von Art. 6 Abs. 1 wiederholt einerseits eine Banalität und ist anderseits ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall eingeschränkt ist, auch dann nicht, wenn ihm nichts vorgeworfen werden kann. Dem ist jedoch nicht so. Es ist ohnehin nicht klar, was «für den Datenschutz verantwortlich» meint. Strafrechtliche Verantwortlichkeit kann es nicht sein, und aufsichtsrechtliche Verantwortlichkeit setzt ebenfalls Kontrollmöglichkeiten voraus. Wird die Verantwortlichkeit schliesslich als zivilrechtliche Haftung verstanden, dann wird mit dieser Regelung eine vom Gesetzgeber nicht vorgesehene Kausalhaftung eingeführt. Hierfür fehlt eine gesetzliche Grundlage. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR.	Mit Blick auf die fehlende gesetzliche Grundlage und die unklare bzw. einen falschen Eindruck erweckende Formulierung ist Abs. 1 von Art. 6 ersatzlos zu streichen.
6	2		Die Bekanntgabe von Personendaten ins Ausland ist in der E-VDSG in Art. 8 ff. (und im nDSG in Art. 16 ff.) geregelt, weshalb Absatz 2 von Art. 6 E-VSDG einerseits systematisch falsch ist und andererseits keine materielle Notwendigkeit dafür besteht. Denn Art. 16 f. nDSG und Art. 9 Abs. 1 nDSG regeln diesen Sachverhalt bereits abschliessend (und Art. 6 Abs. 2 E-VDSG steht damit im Konflikt).	Absatz 2 von Artikel 6 E-VDSG ist ersatzlos zu streichen.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
6	3		Wie an anderen Orten im Erläuternden Bericht ausgeführt (siehe S. 35/87), sollte auch hier – am besten im Verordnungstext selbst – präzisiert werden, dass unter «schriftlich» alle Formen (auch elektronische/digitale) fallen, die den Nachweis durch Text ermöglichen (z.B. ein E-Mail).	Es ist in der E-VDSG klarzustellen, dass unter «schriftlich» alle (physischen und elektronischen/digitalen) Formen fallen, die den Nachweis durch Text ermöglichen.
8	3		Es ist davon auszugehen, dass in Abs. 3 von Art. 8 der Bundesrat angesprochen ist; d.h. ihm (und nicht etwa dem Verantwortlichen) obliegt die Pflicht, die Angemessenheit des Datenschutzes des ausländischen Staates etc. periodisch neu zu beurteilen.	Mindestens der Wortlaut von Art. 8 Abs. 3 ist dahingehend zu präzisieren, dass die Pflicht zur periodischen Neubeurteilung dem Bundesrat obliegt. Noch besser wäre, wenn diese Klärung (Adressat der Bestimmung ist der Bundesrat) für den gesamten Artikel 8 vorgenommen würde.
8	6		Es ist das Verständnis, dass der EDÖB vom Bundesrat vor jedem Entscheid über die Angemessenheit des Datenschutzes von Drittstaaten konsultiert wird.	Der Wortlaut von Art. 8 Abs. 6 ist dahingehend zu präzisieren, dass die Konsultationspflicht nicht dem Verantwortlichen im Einzelfall obliegt, sondern dem Bundesrat im Rahmen dessen genereller Beurteilung der einzelnen Länder etc. Noch besser wäre, wenn generell klargestellt würde, dass sich Art 8 E-VDSG in seiner Gesamtheit an den Bundesrat richtet.
9	1		Die Aufzählung der Anforderungen an Datenschutzklauseln ist untauglich, weil sie nicht zwischen der Art der Übermittlung bzw. Rollen des Exporteurs und Importeurs unterscheidet. Diese sind jedoch für den Inhalt des Vertrags entscheidend, wie beispielsweise die vom EDÖB inzwischen anerkannten Standardvertragsklauseln der Europäischen Kommission (EU SCC) zeigen. So macht es keinen Sinn, Auftragsbearbeiter im Ausland zur Anwendung der Bearbeitungsgrundsätze, zur Information der betroffenen Personen oder zur Wahrung der Rechte der betroffenen Personen zu verpflichten. Sie müssen dem nach nDSG nicht nachkommen, weshalb nicht einzusehen ist, dass sie hierzu vertraglich verpflichtet werden sollen. Zudem fehlt in den Bearbeitungsgrundsätzen (lit. a) der Grundsatz der Transparenz.	Der Anforderungskatalog von Art. 9 Abs. 1 E-VDSG ist ersatzlos zu streichen. Im Minimum ist er anzupassen (siehe auch nachstehend), um unterschiedliche Konstellationen (Controller, Processor) abzudecken. Dabei wäre auch das «mindestens» durch «je nach den Umständen» zu ersetzen. Lit. a ist um den Grundsatz der Transparenz zu erweitern.

			Keine rechtliche Grundlage hat das Erfordernis in lit. d und e, den Namen der Staaten oder der internationalen Organe zu nennen, denen Personendaten bekanntgegeben werden, soweit hiermit Weiterübermittlungen gemeint sind, was nicht klar ist. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Lit. f ist bereits über den Grundsatz der Verhältnismässigkeit abgedeckt und damit redundant. Lit. g geht zu weit, indem es die «berechtigten» Empfänger verlangt. Relevant sind die «Empfänger», also normalerweise die Parteien, welche den Vertrag abschliessen und damit bereits ersichtlich sind. Es fehlen Regelungen zur Meldung von Verletzungen der Datensicherheit, insbesondere soweit die betroffenen Personen zu informieren sind.	Lit d, e, f und g sind ersatzlos zu streichen. Schliesslich sind Meldungen betreffend eine Verletzung der Datensicherheit sind zu regeln.
9	2		In Art. 9 Abs. 2 wird die Pflicht statuiert, dass der Verantwortliche «sicherstellen» muss, dass der Empfänger die Datenschutzklauseln einhält. Diese absolute Formulierung führt zu weit bzw. ist realitätsfern, da der Verantwortliche die Einhaltung der Datenschutzklauseln nicht sicherstellen bzw. nicht garantieren kann.	Das Verb «sicherstellen» ist zu ersetzen, z.B. durch die Formulierung »Der Verantwortliche trägt mit angemessenen Massnahmen Sorge dafür, dass…»
10	1		In Absatz 1 ist verlangt, dass der Verantwortliche «sicherstellt», dass Datenschutzklauseln von den Empfängern der Daten beachtet werden. Diese Beachtung der Klauseln kann der Verantwortliche nicht sicherstellen. Im Erläuternden Bericht wird auf Seite 28/87 ausgeführt, dass Daten-Empfänger „die schweizerischen Datenschutzvorschriften“ einhalten müssen. Die Beachtungspflicht kann sich jedoch nur auf die Einhaltung der Standarddatenschutzklauseln beziehen. Darüber hinaus kann es nur um die Einhaltung von Bestimmungen gehen, die einen gleichwertigen Datenschutz wie in der Schweiz gewährleisten (siehe die Formulierung in Art. 6 Abs. 2 E-VDSG).	Vom Verb «sicherstellen» ist Abstand zu nehmen. Ein möglicher Ersatz könnte «hinwirken» sein oder Sorge tragen» bzw. «dafür sorgen» (analog zur aktuellen Formulierung in Art. 22 Abs. 2 VDSG). Alternativ könnte eine Formulierung gewählt werden, wonach der Verantwortliche angemessene Massnahmen zur Einhaltung der Standardschutzklauseln durch die Datenempfänger treffen muss. Bezüglich Einhaltung der schweizerischen Datenschutzvorschriften ist klarzustellen, dass die Standarddatenschutzklauseln und die Bestimmungen, die einen gleichwertigen Datenschutz wie in der Schweiz gewährleisten, einzuhalten sind (und nicht die schweizerischen Datenschutzvorschriften).

2. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
13	1		Für die in Art. 13 Abs. 1 E-VDSG statuierte Informationspflicht des Auftragsbearbeiters gegenüber der von Datenbeschaffung betroffenen Person gibt es keine gesetzliche Grundlage. Nur dem Verantwortlichen der Datenbearbeitung obliegt eine Informationspflicht. (Art. 19 nDSG). Art. 19 nDSG verlangt eine Information der betroffenen Personen, nicht eine Mitteilung. Für eine Information der betroffenen Person genügt ein Zugänglichmachen. Dies entspricht auch dem Verständnis unter der DSGVO. Durch die Wortwahl «mitteilen» darf keine Verschärfung impliziert werden. Gemäss Verordnungstext sind die Informationen über die Beschaffung von Personendaten in «leicht zugänglicher Form» mitzuteilen. Zugunsten der Rechtssicherheit ist hier in dem Sinne eine Konkretisierung des Verordnungstextes erwünscht, dass als «leicht zugänglich» insbesondere auch die Publikation auf einer Website gilt. In diesem Sinne ist klarzustellen, dass der Erläuternde Bericht fehl geht, wenn darin erwähnt wird, dass eine Kommunikation über eine Website nicht immer genüge. Die im Erläuternden Bericht gemachten Ausführungen sind praxisfremd.	Mangels gesetzlicher Grundlage ist von der in Art. 13. Abs. 1 statuierten Informationspflicht des Auftragsbearbeiters Abstand zu nehmen. Anpassungsvorschlag: «Der Verantwortliche ~~und der Auftragsbearbeiter teilen~~*stellt* die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form *zur Verfügung*~~mit~~. *Als leicht zugänglich gilt eine Information insbesondere dann, wenn sie auf der Webseite des Verantwortlichen abrufbar ist.* ~~Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~»
13	2		Einerseits ist nicht klar, was mit der «Maschinenlesbarkeit von Piktogrammen» gemeint ist, anderseits führt Art. 13 Abs. 2 für die Piktogramme mit der Maschinenlesbarkeit ein neues Formerfordernis ein, für das es keine gesetzliche Grundlage gibt (das nDSG sieht keine Formerfordernisse für Informationen vor).	Mangels gesetzlicher Grundlage und infolge Unverständlichkeit ist Absatz 2 von Art. 13 ersatzlos zu streichen.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
15			Für die in Art. 15 statuierte Pflicht fehlt es in zweierlei Hinsicht an der gesetzlichen Grundlage. Zum einen auferlegt das nDSG – wie bereits vorstehend erwähnt – dem Auftragsbearbeiter keine Informationspflicht. Zum anderen sieht das nDSG nicht vor, dass den Empfängern von Personendaten Informationen zur Aktualität, Zuverlässigkeit und Vollständigkeit der Daten mitgeteilt werden müssen. Zudem ist unklar, was mit «Zuverlässigkeit» der Personendaten gemeint ist.	Art. 15 E-VDSG ist ersatzlos zu streichen.
16			Für die in Art. 16 statuierten Informationspflichten gibt es nicht nur keine gesetzliche Grundlage im nDSG. Vielmehr waren die in Art. 16 der Verordnung enthaltenen Pflichten Bestandteil des Vorentwurfs zum totalrevidierten DSG, wurden aber im Rahmen des Vernehmlassungsverfahrens bewusst gestrichen. Es ist daher nicht korrekt, sie nun auf Verordnungsstufe wieder einzuführen.	Art. 16 E-VDSG ist ersatzlos zu streichen.
18			Es besteht eine grosse Unsicherheit, darüber, bei welchen Bearbeitungen eine Datenschutz-Folgeabschätzung (DSFA) erforderlich ist und bei welchen nicht. Über die VDSG sollte hier mehr Klarheit geschaffen werden. Denkbar wäre, dass analog zu Art. 35 Abs. 4 DSGVO der EDÖB eine Liste publiziert, welche die Bearbeitungen enthält, für die eine oder für die keine DSFA vorzunehmen ist. Alternativ könnte die VDSG Kriterien nennen, die es erlauben zu ermitteln, ob eine DSFA durchgeführt werden muss oder nicht. Wie an anderen Orten im Erläuternden Bericht ausgeführt (siehe S. 35/87), sollte auch hier – am besten im Verordnungstext selbst – präzisiert werden, dass unter «schriftlich» alle Formen (auch elektronische/digitale) fallen, die den Nachweis durch Text ermöglichen. Für die Aufbewahrungsfrist der DSFA gibt es keine gesetzliche Grundlage, weshalb auf die Frist zu verzichten ist.	Formulierungsvorschlag: «[1] *Der EDÖB veröffentlicht eine Liste mit Bearbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist. Er kann zusätzlich eine Liste mit Bearbeitungsvorgängen veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.* [2] Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder *in einer anderen Form, die den Nachweis durch Text ermöglicht, festhalten.* ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~»

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
19			Art. 19 E-VDSG basiert auf Art. 24 nDSG. Zu melden sind demnach Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Die gesetzliche Einschränkung auf Verletzungen, die zu einem hohen Risiko für die Persönlichkeit/die Grundrechte führen, sollte auch in der Verordnungsbestimmung anklingen. Im Erläuternden Bericht finden sich auf Seite 32/87 Ausführungen dazu, was unter «voraussichtlich» (gemäss Art. 24 Abs. 1 nDSG) verstanden werden soll und welches die Folgerungen daraus sind. Dabei wird die Auffassung vertreten, dass bei Verletzungen der Datensicherheit «auch in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, eine Meldung zu erfolgen hat.» Diese Interpretation gibt nach Auffassung der SPA den Willen des Gesetzgebers nicht korrekt wieder. «Voraussichtlich» meint vielmehr, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.	Der Verordnungstext ist dahingehend zu präzisieren, dass Verletzungen der Datensicherheit nur dann gemeldet werden müssen, wenn sie voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Formulierungsvorschlag: «Der Verantwortliche meldet dem EDÖB bei einer *meldepflichtigen* Verletzung der Datensicherheit:» Es ist – im Gegensatz zu den Ausführungen im Erläuternden Bericht – klarzustellen, dass Verletzungen der Datensicherheit nur dann gemeldet werden müssen, wenn die Verletzung höchstwahrscheinlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt – nicht aber dann, wenn ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person nicht ausgeschlossen werden kann.
19	1		Art. 24 nDSG hält fest, dass der Verantwortliche in der Meldung mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen nennt. Dies bedeutet, dass der Verantwortliche zwar zusätzliche Angaben machen kann, aber nicht muss. Den gesetzlichen Anforderungen ist mit der Nennung der Art der Verletzung der Datensicherheit, deren Folgen und der ergriffenen oder vorgesehenen Massnahmen Genüge getan. Es gibt damit keine gesetzliche Grundlage, um auf Verordnungsebene den Katalog der mitzuteilenden Angaben zu erweitern. Überdies ist lit. e falsch formuliert: Die «allfälligen Risiken» beinhalten bereits die Folgen für die	Die in Abs. 1 lit. b-d zusätzlich verlangten Angaben sind aus dem Verordnungstext zu entfernen. Lit. e von Art, 19 Abs. 1 ist wie folgt neu zu formulieren: «die Folgen *der Datenbearbeitungen* für die

			betroffenen Personen. Richtig müsste es heissen «die Folgen der Datenbearbeitungen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht». Auch in lit. f müsste nicht von den «Folgen», sondern vom «Risiko» die Rede sein. Gemildert werden kann entweder das Schadensausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem «Risiko» entspricht). Wünschenswert wäre schliesslich eine «de minimis»-Regelung, die jene Fälle ausschliesst, in welchen der EDÖB nicht wirklich etwas tun kann oder will (z.B. eine problematische E-Mail geht an den falschen Empfänger und ein Missbrauch durch diesen ist möglich). Damit können auch die Ressourcen des EDÖB geschont werden.	betroffenen Personen, *von welchen ein hohes Risiko ausgeht*» Es sollte zudem eine «de minimis»-Regelung vorgesehen werden, welche Fälle erfasst, in denen trotz eines hohen Risikos für eine betroffene Person sinnvollerweise nicht gemeldet werden muss.
19	3		Art. 24 Abs. 4 nDSG verlangt, dass der Verantwortliche die betroffene Person informiert, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Eine Information an die betroffene Person ist damit nur in den beiden genannten Fällen gesetzlich verlangt. Dagegen wird in Abs. 3 von Art. 19 E-VDSG ohne Einschränkungen verlangt, dass betroffene Personen zu informieren sind. Für diese Ausweitung der Informationspflicht fehlt es an der gesetzlichen Grundlage, weshalb davon Abstand zu nehmen ist.	In Abs. 3 von Art. 19 E-VDSG ist die Informationspflicht wie folgt einzuschränken: «~~Der Verantwortliche teilt den betroffenen Personen~~ *Wenn der Verantwortliche verpflichtet ist, die betroffenen Personen zu informieren, teilt er ihnen* in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit.
19	5		Für die in Abs. 5 postulierte Dokumentationspflicht und für die Aufbewahrungspflicht gibt es keine gesetzliche Grundlage, weshalb darauf zu verzichten ist. Die gesetzliche Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten ist genügend.	Abs. 5 von Art. 19 E-VDSG ist ersatzlos zu streichen.

3. Kapitel: Rechte der betroffenen Person

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
20	1 und 2		Im Erläuternden Bericht wird ausgeführt (siehe S. 35/87), dass zur schriftlichen Form auch die elektronische Form gehört. Das sollte im Verordnungstext selbst präzisiert werden, indem explizit festgehalten wird, dass unter «schriftlich» alle Formen fallen, die den Nachweis durch Text ermöglichen (so z.B. auch ein E-Mail). Der Erläuterungsbericht erwähnt zudem die «digitale Form» ohne klarzustellen, ob diese als «elektronische Form» i.S. von «schriftlich» verstanden wird. Hierzu bedarf es einer Klärung.	Vorgeschlagene Ergänzung: «schriftlich oder in einer anderen Form, die den Nachweis durch Text ermöglicht» Es ist eine Klärung des Begriffs «digitale Form» vorzunehmen.
20	2		Zur Präzisierung sollte in Abs. 2 von Art. 20 E-VDSG festgehalten werden, dass die Einsichtnahme vor Ort auch dann eine gültige Erfüllung der Auskunftspflicht des Verantwortlichen darstellt, wenn aufgrund von berechtigten Interessen des Verantwortlichen eine schriftliche Auskunft nicht zumutbar ist. Im Erläuternden Bericht (S. 35/87) wird ausgeführt, dass die betroffene Person bei der Einsichtnahme an Ort und Stelle gleichwohl die Möglichkeit haben müsse, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Dies entspricht jedoch nicht den Intentionen des Gesetzgebers, wonach im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten besteht. Der Gesetzgeber hat die Auskunftspflicht bewusst auf die Mitteilung der „bearbeiteten Personendaten als solche“ (Art. 25 Abs. 2 lit. b nDSG) beschränkt. Damit wird die Auskunftserteilung in aggregierter Form ermöglicht. Dies sollte in der VDSG ausdrücklich festgehalten werden.	Präzisierung von Art. 20 Abs. 2 in dem Sinne, dass die Einsichtnahme vor Ort eine gültige Erfüllung der Auskunftspflicht des Verantwortlichen darstellt. Es ist – im Gegensatz zu den Ausführungen im Erläuternden Bericht – klarzustellen, dass die betroffene Person bei der Einsichtnahme an Ort und Stelle keinen Anspruch auf Herausgabe von Akten bzw. auf das Anfertigen von Fotokopien bestimmter Akten in ihrem Dossier hat. In der VDSG ist ausdrücklich festzuhalten, dass die Auskunftspflicht auf die Mitteilung der bearbeiteten Personendaten als solche beschränkt ist.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
20	3		Die Anforderung, wonach die Auskunft für die betroffene Person verständlich zu sein hat, ergibt sich bereits aus dem allgemeinen Grundsatz von Treu und Glauben, womit sie im Verordnungstext obsolet ist.	Abs. 3 von Art. 20 E-VDSG ist ersatzlos zu streichen. Eventualiter ist zu präzisieren, dass die Anforderung, wonach die Auskunft für die betroffene Person verständlich zu sein hat, an einem objektiven Massstab zu messen ist. Subjektive Umstände der betroffenen Person dürfen keine Rolle spielen.
20	5		Für die in Abs. 5 von Art. 20 E-VDSG statuierte Dokumentationspflicht fehlt es an der gesetzlichen Grundlage, womit auf diese Pflicht zu verzichten ist. Dies gilt umso mehr, als der Verantwortliche seine Einschränkungsgründe bereits gestützt auf Art. 26 Abs. 4 nDSG gegenüber den betroffenen Personen angeben muss. Um sich im Falle einer Klage oder einer Anzeige zu verteidigen, wird er diese auch aufbewahren.	Absatz 5 von Artikel 20 E-VDSG ist ersatzlos zu streichen.
22			Es ist in der Verordnung klarzustellen, wann die Auskunftserteilungs-Frist von 30 Tagen zu laufen beginnt. Dabei sind u.a. folgende Fälle zu berücksichtigen: • Die Frist beginnt nicht mit Eingang des Begehrens zu laufen, sondern erst wenn der Antragsteller einwandfrei identifiziert werden konnte (wenn z.B. eine Ausweiskopie fehlt, läuft die Frist noch nicht). • Die Frist beginnt erst zu laufen, wenn das Begehren keiner Präzisierung mehr bedarf. Wenn aus dem Auskunftsbegehren beispielsweise nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst nach erfolgter Klarstellung zu laufen. • Wenn die Auskunftserteilung nicht kostenlos erfolgen kann (Art. 23 Abs. 1 E-VDSG), muss die betroffene Person vor der Auskunftserteilung über die Höhe der Kostenbeteiligung in Kenntnis gesetzt werden (Art. 23 Abs. 3 E-VDSG). Sie kann dann ihr	In Artikel 22 E-VDSG ist klar zu bezeichnen, wann die dreissigtägige Frist für die Auskunftserteilung zu laufen beginnt.

			Gesuch innert zehn Tagen zurückziehen. Die Frist von 30 Tagen für die Auskunftserteilung beginnt damit erst nach Ablauf der Rückzugsfrist zu laufen.	
23	2		Gemäss Art. 25 Abs. 6 nDSG kann der Bundesrat eine Beteiligung an den Kosten der Auskunftserteilung vorsehen, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. Bereits «normale» Auskunftsbegehren (also solche, die keinen unverhältnismässigen Aufwand im Sinne des Gesetzgebers verursachen) dürften regelmässig einen Aufwand verursachen, der deutlich über dem Betrag vom CHF 300 liegt, der in Art. 23 Abs. 2 E-VDSG vorgesehen ist. Das bedeutet, dass über das Normale hinausgehende Begehren rasch einmal einen Aufwand von vielen tausend oder zehntausend Franken verursachen können. Hierfür nur eine Kostenbeteiligung von CHF 300 vorzusehen, wird der gesetzlichen Bestimmung von Art 25 Abs. 6 nDSG nicht gerecht, da der Kostendeckel in keinem vernünftigen Verhältnis zum effektiven Aufwand steht. Die vorgesehene starre Begrenzung bei CHF 300 ist daher durch eine Regelung zu ersetzen, welche den im Einzelfall konkret anfallenden Kosten besser bzw. angemessen gerecht wird.	Die Beteiligung der betroffenen Person an den Kosten der Auskunftserteilung ist in der VDSG im Verhältnis zum für die Auskunftserteilung angefallenen Aufwand zu regeln. Formulierungsvorschlag: «Die Angemessenheit der Kostenbeteiligung misst sich am tatsächlich für die Auskunftserteilung entstandenen Aufwand»
24			Die Datenportabilität wurde erst in der parlamentarischen Beratung ins nDSG eingefügt. Art. 28 nDSG ist dabei insofern im DSG sachfremd, als damit keine datenschutzrechtlichen Interessen verfolgt werden. Die in Art. 24 E-VDSG vorgesehene analoge Anwendung der Art. 20 bis 23 E-VDSG auf die Datenherausgabe und die Datenübertragung ist daher nicht passend bzw. greift zu kurz.	Von den in Artikel 24 E-VDSG vorgenommenen Verweisen ist abzusehen. Wo nötig sind spezifische bzw. eigenständige Ausführungsbestimmungen zur Datenportabilität zu erlassen.

4. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
25			Die Kompetenzen des Datenschutzbeauftragten nach DSGVO und des Datenschutzberaters nach nDSG/ E-VDSG sind unterschiedlich. Die Abgrenzung zwischen dem Datenschutz*berater* und dem Verantwortlichen ist nicht klar, wenn ein Unternehmen nach Art. 37 DSGVO bereits über einen Datenschutz*beauftragten* verfügt.	Es wäre eine Klärung auf Verordnungsstufe für diejenigen Konstellationen sinnvoll, in denen ein Unternehmen bereits über einen Datenschutzbeauftragten nach DSGVO verfügt.
25	1		Aus dem nDSG ergibt sich keine Pflicht zur Ernennung einer Datenschutzberaterin/eines Datenschutzberaters. Die in Art. 25 Abs. 1 enthaltene Formulierung «Die Datenschutzberaterin […] muss folgende Aufgaben wahrnehmen» suggeriert jedoch, dass eine solche Pflicht besteht. Die Formulierung ist daher anzupassen.	Formulierungsvorschlag: «Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen *nimmt* ~~muss~~ folgende Aufgaben *wahr* ~~wahrnehmen~~:»

6. Kapitel: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
45			Wird der EDÖB gegenüber einer privaten Person tätig, so soll er diese vorab über die voraussichtlichen Gebühren für seine Tätigkeit informieren.	Formulierungsvorschlag: «Der Verantwortliche ist über die erwartete Höhe der Gebühren vorab in Kenntnis zu setzen»

Wir danken Ihnen für die Prüfung unserer Ausführungen sowie für die Berücksichtigung unserer Überlegungen und Anliegen. Gerne stehen wir Ihnen für Rückfragen bzw. zur Erläuterung unserer Eingaben zur Verfügung.

Freundliche Grüsse
Swiss Payment Association

Roland Zwyssig
Präsident

Dr. Thomas Hodel
Geschäftsführer

Überall für alle
SPITEX
Schweiz

Spitex Schweiz · Effingerstrasse 33 · 3008 Bern

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Per E-Mail an:
jonas.amstutz@bj.admin.ch

Bern, 8. Oktober 2021

Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG): Stellungnahme Spitex Schweiz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

In Ihrem Schreiben vom 23. Juni 2021 haben Sie uns eingeladen in vorgenannter Angelegenheit Stellung zu nehmen. Gerne geben wir Ihnen fristgerecht Antwort und bedanken uns für die Möglichkeit zur Stellungnahme.

I. Ausgangslage

Die DSG-Totalrevision umfasst zum einen eine Totalrevision des DSG (E-DSG), zum andern eine Teilrevision weiterer Bundesgesetze. Das Parlament hat die Vorlage des Bundesrates in zwei Etappen aufgeteilt. In der ersten Etappe wurde nur eine EU-Richtlinie zum Datenschutz in Strafsachen (SDSG) umgesetzt und am 1.3.2019 in Kraft gesetzt. In einer zweiten Etappe hat das Parlament das neue Datenschutzgesetz (nDSG) am 25.9.2020 verabschiedet. Die vorliegende Vernehmlassung über das Umsetzungsrecht des revidierten DSG (Vorentwurf der revidierten Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)) wurde am 23.6.3021 eröffnet. Sie dauert bis am 14.10.2021.

II. Grundzüge der vorliegenden Vernhemlassungsantwort

Im Rahmen des vorliegenden Verfahrens haben die Verbände CURAVIVA Schweiz, INSOS Schweiz, senesuisse und Spitex Schweiz eng zusammengearbeitet, so dass ihre Vernhemlassungsantworten inhaltlich übereinstimmende Standpunkte vertreten.

Da es sich im Rahmen der vorliegenden Vernehmlassung nur noch um die Gestaltung des Umsetzungsrechts einer bereits erfolgten Gesetzesrevision handelt, ist der Ermessenspielraum für Anpassungen der neuen Gesetzgebung sehr begrenzt.

Die vorliegende Vernehmlassungsantwort begrenzt sich auf die für die Institutionen und Strukturen für Menschen mit Unterstützungsbedarf relevanten Punkte der vom Bundesrat vorgeschlagene VDSG-Revision.

In der vorliegende Vernehmlassungsantwort wird in erster Linie darauf beachtet, dass die vom Bundesrat vorgeschlagenen Umsetzungsmodalitäten des revidierten Datenschutzgesetzes möglichst schlank, praxisnah und anwendungsfreundlich für die Betriebe bleiben. Das ist nicht selbstverständlich im Rahmen eines Gesetzgebungsprozesses, der nicht besonders darauf ausgerichtet ist: Dieser strebt offensichtlich vor allem eine sehr genaue und umfangreiche Einhaltung des Datenschutzes an.

Des Weiteren beantragt die vorliegende Vernehmlassungsantwort, wo es möglich ist, eine möglichst konkrete, zugängliche und auch finanziell günstige Unterstützung der Betriebe durch die zuständigen staatlichen Stellen – vor allem durch den Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu ermöglichen.

Die in der vorliegenden Vernehmlassungsantwort vertretenen Standpunkte berücksichtigen gleichwohl die Wichtigkeit eines zielführenden Datenschutzes: Allgemein wird davon ausgegangen, dass die Betriebe oftmals heikle Daten bearbeiten, deren Bekanntgabe ein hohes Risiko für die betroffenen Personen von Unterstützungsleistungen aufweisen können; deswegen soll an einem strikten Datenschutz nicht gerüttelt werden.

Auch wird in der vorliegenden Vernehmlassungsantwort beantragt, dass etwas stumpfe Begriffe und Abgrenzungen präziser umschrieben werden – dies im Sinne einer möglichst klaren Umsetzungshilfe für die betroffenen Betriebe.

III. Relevante Bestimmungen der E-VDSG für die ambulanten und stationären Betriebe für Personen mit Unterstützungsbedarf

E-VDSG	**Kommentar**	**Beantragte Neuformulierung**
Art. 1 Abs. 1	Die vorgeschlagene Umschreibung ist im Grundsatz zu begrüssen. Sie ergänzt und konkretisiert sinnvollerweise Artikel 8 Absatz 1 nDSG. Zu begrüssen ist, dass sie möglichst schlank und angesichts der stetigen technischen Entwicklungen flexibel, praxisnah und anwendungsfreundlich gehalten worden ist. Weil sie sehr allgemein formuliert ist, braucht es aber entsprechenden Deutungs- und Umsetzungshilfen für die Praxis.	- Es müssen seitens EDÖB möglichst bald Dokumente geschaffen werden, welche den Betrieben die Praxisumsetzung vereinfachen.
Art. 1 Abs. 2	Die Abstände zwischen den vorzunehmen Überprüfungen sollten präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Was genau „angemessene Abstände“ sind, hängt selbstverständlich von den Besonderheiten des konkreten Anwendungsfalls ab (S. 17 im erläuternden Bericht: «[…] bei der Bestimmung der Massnahmen selbstredend die Umstände des Einzelfalls massgeblich [bleiben]»). Während die Datenbearbeiter <u>inhaltlich</u> grossen Freiraum für die Bestimmung ihrer konkreten Massnahmen brauchen, sollte <u>zeitlich</u> zumindest eine konkrete Anforderung gelten, um die Sicherheit zu gewährleisten. Als sinnvoll erscheint uns eine mindestens jährliche Überprüfung.	[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen<u>, jedoch mindestens einmal pro Jahr</u> zu überprüfen.

Art. 2	Diese präzise Auflistung der Schutzziele macht Sinn: Sie stellt eine praxisorientierte ‚Gedächtnisstütze' für die Verantwortlichen und die Auftragsbearbeiter dar, was im Rahmen ihrer Konkretisierung zu berücksichtigen ist. Wichtig ist eine gute Anwendbarkeit in der Praxis (Seite 17 des Berichts: „In Anwendung der Verhältnismässigkeit sind ausgehend […] von dieser Auflistung der Schutzziele] die organisatorischen und technischen Massnahmen des Einzelfalls zu bestimmen."). Gleichzeitig zeigt diese Auflistung die Komplexität der Anforderungen an eine gesetzkonforme Datenbearbeitung und -sicherheit auf - mit dem damit verbundenen Aufwand. Aus diesem Grund ist eine möglichst konkrete und für Schweizer Betriebe auch unentgeltliche Unterstützung der Datenschutzverantwortlichen durch die zuständigen Behörden (insbesondere das EDÖB), vorzusehen. So können die Umsetzungskosten für Wirtschaft und Gesellschaft minimiert und angemessene Datensicherheit auf allen Ebenen geschaffen werden.	- Für eine optimale und kostengünstige Umsetzung ist darauf zu achten, dass Schweizer Unternehmen einen guten und kostengünstigen Zugang zum EDÖB erhalten (vgl. auch Art. 45 Abs. 2).
Art. 3	Welche „Massnahmen" im vorliegenden Rahmen berücksichtigt werden sollen und ob ein Risiko als hoch oder begrenzt eingeschätzt werden soll, dürfte in der Praxis oftmals schwierig zu beurteilen sein, denn Artikel 8 nDSG führt auch keine präziseren Anhaltspunkte über die Art der infrage stehenden Massnahmen. Dies entspricht zwar einer flexiblen, bedarfsorientierten und dem neusten technischen Stand angepassten Umsetzung des Datenschutzes, macht aber dessen Realisierung in der Praxis schwierig. In diesem Sinne ist die Präzisierung der Inhalte der Protokollierung (gemäss Abs. 3) an sich konsequent und kongruent. Sie weist aber einen hohen Detaillierungsgrad auf, der einen entsprechend hohen Umsetzungsaufwand, eine Unübersichtlichkeit und mögliche Verwechslungsrisiken mit sich bringt. Es ist festzustellen, dass gerade bei der *automatisierten* Bearbeitung von Personendaten die Anforderung einer detaillierten Protokollierung einen beträchtlichen Teil der Vorteile der Automatisierung beraubt: Der zeitliche und administrative Aufwand wird dadurch erheblich vergrössert. Trotzdem erscheint uns eine Protokollierung richtig, sofern keine anderen Massnahmen das gleiche Ziel mit weniger Aufwand erreichen können. *<u>Antrag:</u>* Alternativen zur Protokollierung als Massnahmen zum Datenschutz sollen im E-VDSG ausdrücklich vorgesehen und auch aufgezählt werden – wie etwa die physische/räumliche Sicherung der Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.	In Art. 3 Abs. 1 müssen Alternativen zur im Entwurf vorgesehenen (komplexen) Protokollierung – ausdrücklich vorgesehen und auch aufgezählt werden, namentlich Zugriffskontrollen, die physische/räumliche Sicherung der Daten, das Aufstellen fehlertoleranter Systeme und Massnahmen der Datensicherung.
Art. 4 Abs. 2	Weil in sehr vielen Fällen eine automatisierte Bearbeitung von besonders schützenswerten Personendaten erfolgt, sind die von dieser Bestimmung gestellten Anforderungen als zu aufwendig und vielfach unnötig zu qualifizieren. Sie bringen für die betroffenen Datenbearbeiter unangemessen hohe Kosten mit sich. Deswegen ist diese Auflistung zu kürzen: Die Buchstaben d, e und j sollen ersatzlos gestrichen werden, weil sie unnötige zusätzliche Anforderungen und	[2] Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die

	Präzisierungen darstellen, die den administrativen Aufwand für die Betriebe verschärfen, ohne dass daraus ein entsprechender Nutzen entsteht. Buchstabe i soll gekürzt werden: Er weist einen Detaillierungsrad mit entsprechenden Umsetzungskosten auf, der in keinem vernünftigen Verhältnis zu seinem Nutzen steht. Hingegen werden Buchstaben a, b, c, f und g ausdrücklich begrüsst, da sie zentrale Massnahmen zur Gewährleistung der Datensicherheit darstellen. Ihre Einhaltung genügt, um dem Datenschutz gerecht zu werden. Auch Buchstabe h wird begrüsst, weil eine stets angestrebte Datenminimierung das beste Mittel darstellt, um sowohl den Schutz der Privatsphäre als auch die Verminderung des mit jeglichem Datenbearbeitung verbundenen administrativen Aufwands zu erreichen.	Kriterien zur Festlegung dieser Dauer; d. ~~zur internen Organisation~~; e. ~~zur Herkunft der Personendaten und zur Art ihrer Beschaffung~~; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den ~~Datenbearbeitungsverfahren, insbesondere den~~ Verfahren bei der Speicherung, ~~Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung,~~ Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. ~~zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.~~
Art. 4 Abs. 3	Wie gemäss obigem Antrag zu Art. 1 Abs. 2 sollten auch hier die zeitlichen Abstände zwischen den vorzunehmen Aktualisierungen präziser angegeben werden, sonst drohen Rechtsunsicherheit und Streitigkeiten. Deswegen wird hier beantragt, dass die Aktualisierungen mindestens einmal jährlich stattfinden: Dieser Zeitabstand stellt eine präzise, zugleich realistische und daher auch anwendungsfreundlich Leitplanke dar.	[3] Die private Person muss das Reglement ~~regelmässig~~ in angemessenen Abständen, jedoch mindestens einmal pro Jahr, aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.
Art. 6 Abs. 2	Die in dieser Bestimmung gestellten Anforderungen an die Verantwortlichen betreffend dem DSG nicht unterstellten Datenbearbeiter sind offensichtlich zu hoch. Von einem Verantwortlichen kann vernünftigerweise nicht verlangt werden, dass er Kenntnis der vielen potenziell relevanten Gesetzesbestimmungen und der möglichen Abhilfe-Lösungen hat. Wenn schon ist es die Pflicht von Gesetzgeber und Verwaltung, den Datenschutz so auszugestalten, dass dieser – wo nötig und sinnvoll – überall für alle Betroffenen gleichermassen gilt. Diese Pflicht den einzelnen Verantwortlichen aufzubürden, wie der Bundesrat es vorschlägt, führt zu enormer Unsicherheit und Aufwand. Deswegen ist dieser Absatz ersatzlos zu streichen.	~~[2] Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.~~
Art. 8 Abs. 1	Aus der Formulierung dieser Bestimmung geht überhaupt nicht klar hervor, wer für die Beurteilung der Angemessenheit des Datenschutzes in einem anderen Staat zuständig ist. Aus dem erläuternden Bericht hingegen schon (S. 25 ff): Der	[1] Werden Personendaten ins Ausland bekanntgegeben, so müssen ~~bei der~~ anlässlich einer regelmässigen Beurteilung durch

	Bundesrat ist zuständig. Der Klarheit halber sollte diese Zuständigkeit in Art. 8 E-VDSC eindeutig geregelt werden, sonst besteht das Risiko, dass sich private Akteure dafür verantwortlich halten – was ihren Aufwand erheblich erhöhen würde.	den Bundesrat, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden: […]
Art. 8 Abs. 3	Die Abstände zwischen den vorzunehmenden Beurteilungen sollen präziser angegeben werden. Deswegen wird auch hier beantragt, dass die Beurteilungen mindestens einmal jährlich stattfinden müssen.	[3] Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch, jedoch mindestens einmal pro Jahr, neu beurteilt.
Art. 9 Abs. 1	Die von Art. 9 E-VDSG gestellten Anforderungen erreichen ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Zwar sind diese Anforderungen für das Ziel des Datenschutzes konsequent, sie verursachen aber hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden. Nämlich Bst. b, c, g, h sowie i sind offensichtlich unnötig; Ihre Anwendung wäre unverhältnismässig aufwendig. Die anderen Bestimmungen genügen, um die «spezifischen Garantien» zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.	[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen die Datensicherheit mindestens die folgenden Punkte regeln: […] ~~b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen~~ ~~c. die Art und der Zweck der Bekanntgabe von Personendaten;~~ ~~[…]~~ ~~g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger;~~ ~~h. die Massnahmen zur Gewährleistung der Datensicherheit;~~ ~~i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;~~ […]
Art. 10	Wir begrüssen, dass der EDÖB eine Liste von Standard-Datenschutzklauseln veröffentlicht, um den Aufwand für die Betroffenen zu reduzieren und eine gewisse Vereinheitlichung der Schutzklauseln zu erreichen.	-

Art. 15	Bei der Anwendung dieser Bestimmung ist darauf zu achten, dass die Anforderungen an den Detaillierungsgrad der mit der Bekanntgabe von Personendaten verbundenen Informationen nicht zu umfangreich ausfallen soll. Meistens werden sich die zum Datenschutz benötigten Informationen aus den Daten oder den Begleitumständen selbst ergeben.	-
Art. 18	Nach unserer Einschätzung reicht es aus, wenn *nach Beendigung der Datenbearbeitung* (was bei entsprechenden Gerichtsverfahren bereits Jahre dauern kann) eine Aufbewahrung für ein Jahr statt zwei Jahre stattfindet.	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während ~~zwei Jahren~~ einem Jahr nach Beendigung der Datenbearbeitung aufbewahrt werden.
Art. 20	Die vorgesehene Dreifachlösung (schriftlich, mündlich oder durch Einsichtnahme an Ort und Stelle) erscheint als sehr sinnvoll. So kann für Menschen mit gewissen Krankheiten oder Beeinträchtigungen eine geeignete Lösung gefunden werden. Für gewisse Fälle, wie urteilsunfähige, an Demenz erkrankte oder weitere kognitiv behinderte Menschen dürfte die Anforderung in Abs. 3 kaum einzuhalten sein. Deshalb ist für diese Fälle eine Präzisierung aufzunehmen.	[3] Die Auskunft muss für die betroffene Person verständlich sein, soweit dies im Rahmen des kognitiven Zustands möglich ist.
Art. 22	Die Frist von 30 Tagen ab Eingang des Begehrens um Dateneinsicht erscheint uns als vernünftig. Es stellt sich einzig die Frage, ob nicht die Gerichtsferien berücksichtigt werden sollten (namentlich die Sommermonate und Weihnachten, wegen vieler Absenzen).	-
Art. 23	Bei unverhältnismässig aufwändigen Auskunftserteilungen erscheint uns die auf 300 Franken angesetzte Obergrenze als viel zu tief. Wenn damit mehrere Arbeitstage an Aufwand anfallen, wäre nicht einmal ein Bruchteil der Kosten auf die Gesuchstellenden gedeckt. Der Betrag sollte – auch gerade als Schutz vor querulatorischen Begehren – auf mindestens 1'000 Franken erhöht werden, um tatsächlich abschreckend wirken zu können.	[1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. [2] Die Beteiligung beträgt maximal ~~300~~ 1'000 Franken.
Art. 25	Die Datenschutzgesetzgebung weist eine hohe Komplexität auf; deshalb sind ihre Anforderungen in der Praxis nicht immer einfach einzuhalten. Deswegen ist es sehr sinnvoll, Datenschutzberatende einzusetzen und die konkreten Modalitäten zu deren Einsatz im Sinne dieser Bestimmung festzulegen. Die Inhalte sind zu begrüssen, wie sie in dieser Bestimmung vorgeschlagen sind.	-
Art. 26 Bst. a + b	Die hier definierte und sehr sinnvolle Ausnahme einer Pflicht zur Führung eines Bearbeitungsverzeichnisses würde bei zahlreichen Betrieben nicht zur Anwendung kommen, weil • in vielen Fällen die Betriebe besonders schützenswerte Personendaten in grossem Umfang bearbeiten; • aus einer Interpretation von Art. 20 Abs. 4, Art. 26 Abs. 3, Art. 31 Abs. 2 Bst. b nDSG hervorgeht, dass Art. 26 eVSDG auch Betriebe mit weniger als 250 Mitarbeitenden angewendet werden soll, wenn sie einem Konzern zugehören, der insgesamt mindestens 250 Mitarbeitende beschäftigt.	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:

	Um Rechtssicherheit zu gewährleisten und keinen unnötigen Aufwand für kleinere Betriebe (namentlich auch gerade im Gesundheitswesen) zu schaffen, ist eine Anpassung wichtig. Während wir die Unterstellung von Teilen der Konzerne nachvollziehen können, erscheint uns die «Bearbeitung von besonders schützenswerten Daten in grossem Umfang» als zu wenig präzise Konkretisierung. Wir beantragen deshalb eine Präzisierung, was unter «grossem Umfang» zu verstehen ist, nach unserer Ansicht wäre die Schwelle etwa bei 1000 Datensätzen festzusetzen. Diesfalls erhält auch die Führung eines Verzeichnisses aber auf freiwilliger Basis mehr Gewicht, sie kann insbesondere bei regelmässiger Bearbeitung von Personendaten eine nützliche und einfache Tätigkeitsunterstützung darstellen: Dadurch können das Beibehalten eines Überblicks der Bearbeitungstätigkeiten und auch die Einhaltung anderer Verpflichtungen erleichtert werden.	a. Es werden umfangreich (mindestens 1000 Datensätze) besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.
Art. 45 Abs. 2	Aus unserer Sicht ist absolut unverständlich, warum eine nationale Behörde für die Dienstleistung im Bereich des der ganzen Bevölkerung dienenden Datenschutzes solch hohe Kostensätze von 150 bis 350 Franken verlangen soll. Dies schreckt geradezu ab, diese sinnvollen Dienstleistungen zu beziehen, welche einer guten Umsetzung der Gesetzgebung dienen. Es ist unverständlich, dass für die Dienstleistungen der Verwaltung solche Preise wie bei spezialisierten Anwaltskanzleien verrechnet werden. Als ganz besonders stossend empfinden wir solche Honorare im Bereich der nach KVG zugelassenen Leistungserbringer. Bei diesen Gesundheitsbetrieben handelt es sich um Institutionenen, bei welchen der Datenschutz wegen hoch sensibler Daten besonders wichtig ist. Es wäre falsch, diese mit hohen Stundensätzen vom Bezug der sinnvollen Unterstützung seitens EDÖB abzuschrecken. Diese Betriebe sind denn mit den neuen Regelungen auch besonders stark herausgefordert und eine gute Umsetzung ist im Interesse der Behörden und der Bevölkerung. Diese Belastung ist umso fragwürdiger, als die öffentliche Hand im Endeffekt und in vielen Fällen, die dadurch verursachten Defizite ausgleichen soll: Mit einer Hand wegnehmen, was mit der anderen gegeben wird, macht betriebswirtschaftlich keinen Sinn und verursacht einen sinnlosen administrativen Aufwand. Die Zutrittsschwelle zum EDÖB ist niedrig zu halten, ganz besonders auch zur Überprüfung der Angemessenheit von Kodizes (Art. 59 Abs. 1 Bst. a nDSG) oder die Genehmigung von Standarddatenschutzklauseln (Art. 59 Abs. 1 Bst. b nDSG). Im Sinne einer rechtmässigen Umsetzung der komplexen neuen Datenschutzgesetzgebung sollte das Anrufen des EDÖB nicht durch das Erheben von Gebühren entgegengewirkt werden. Ganz besonders für den Bereich der Gesundheitsbetriebe muss deshalb eine Ausnahme geschaffen werden, welche vernünftige Stundenansätze vorsieht.	[2bis] Für Leistungserbringer nach Art. 35 Abs. 2 KVG wird auf die Erhebung von Kosten verzichtet. Alternativ: [2bis] Für Leistungserbringer nach Art. 35 Abs. 2 KVG gilt ein Stundenansatz von 50 bis 100 Franken.

Wir danken Ihnen für die Prüfung und Berücksichtigung unserer Anliegen. Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse,

SPITEX SCHWEIZ

M. Pfister

C. Kooijman

Marianne Pfister
Geschäftsführerin

Cornelis Kooijman
Stv. Geschäftsführer, Leiter
Grundlagen und Entwicklung

Spitex Schweiz
Geschäftsstelle
www.spitex.ch

Effingerstrasse 33
3008 Bern

Telefon 031 381 22 81
info@spitex.ch

Nationale Spitex-Nummer
0842 80 40 20

Schweizerische Zahnärzte-Gesellschaft
Société suisse des médecins-dentistes
Società svizzera odontoiatri
Swiss Dental Association

Sekretariat/Secrétariat
Münzgraben 2, Postfach, CH-3001 Bern
Telefon 031 313 31 31, Fax 031 313 31 40
E-mail: sekretariat@sso.ch
CHE 105.830.570 MWST

per E-Mail an:
jonas.amstutz@bj.admin.ch
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Bern, 12. Oktober 2021

Stellungnahme SSO betreffend

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Gerne machen wir von der Möglichkeit Gebrauch, zum obgenannten Entwurf Stellung zu nehmen.

Allgemeine Bemerkungen

Die Schweizerische Zahnärzte-Gesellschaft SSO ist die Berufs- und Standesorganisation der in der Schweiz tätigen Zahnärztinnen und Zahnärzte. Sie vertritt 3500 Praxisinhaber und insgesamt 5800 Zahnärzte. Dabei handelt es sich mehrheitlich um Mikro- und Kleinunternehmen. Die Regulierungskosten treffen die Zahnärztinnen und Zahnärzte deshalb besonders schwer. Grössere Unternehmen können sich eine mit administrativen Aufgaben betraute Stelle eher Leisten als Mikro- und Kleinunternehmen.

Die Zahnärztinnen und Zahnärzte nehmen den Datenschutz ernst. Trotzdem darf die Arbeit nicht durch unnötige administrative Belastungen erschwert werden.

Der Verordnungsentwurf enthält verschiedene Punkte, bei denen eine gesetzliche Grundlage fehlt, d.h. diese sind im neuen Datenschutzgesetz nicht vorgesehen und somit zu streichen:

- Pflicht Privater ein Bearbeitungsreglement zu führen
- Pflicht, Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der bekanntgegebenen Personendaten und deren Berichtigung, Löschung usw. zu informieren
- Pflicht, Dokumentationen zu führen und aufzubewahren

Zu den einzelnen Bestimmungen

Zu Art. 1 Abs. 2

Zu prüfen sind die Massnahmen eigentlich nicht "in angemessenen Abständen", sondern "in angemessener Weise". Ohne Änderung der Risikofaktoren müssen die Massnahmen nicht überprüft werden.

Änderungsantrag:

Art. 1 Abs. 2

Die Massnahmen sind ~~**über die gesamte Bearbeitungsdauer hinweg**~~ in ~~**angemessenen Abständen**~~ **angemessener Weise** zu überprüfen**.**

Zu Art. 2

Die Massnahmen müssen die Schutzziele nicht erreichen, sondern sie anstreben. Eine absolute Sicherheit kann nicht verlangt werden.

Änderungsantrag:

Art. 2 Schutzziele

Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele ~~**erreichen**~~ **anstreben**: ...

Zu Art. 3

Es ist unklar, wie sich die hier festgehaltene Protokollierungs- und Aufbewahrungspflicht aus dem Gesetz herleiten lässt.

Zu Art. 4

Es fehlt eine gesetzliche Grundlage für das Erfordernis eines Datenbearbeitungsreglement. Auf ein solches hat der Gesetzgeber explizit zu Gunsten eines Bearbeitungsverzeichnisses verzichtet.

Antrag: Art. 4 ist zu streichen.

Zu Art. 6 Abs. 1

Der Verantwortliche kann niemals sicherstellen, dass Daten vertrags- und gesetzesgemäss bearbeitet werden – er kann nur dazu Sorge tragen.

Zu Art. 13 Abs. 1

Es besteht keine gesetzliche Grundlage für eine Meldepflicht des Auftragsbearbeiters. Zudem soll für den Verantwortlichen

Änderungsantrag:

Art. 13 Modalitäten der Informationspflichten

1 Der Verantwortliche ~~**und der Auftragsbearbeiter teilen**~~ **teilt** die Information ….

Zu Art. 15

Auch hier fehlt es an einer gesetzlichen Grundlage.

Antrag: Art. 15 ist ersatzlos zu streichen

Zu Art. 16

Auch hierzu fehlt es an einer gesetzlichen Grundlage.

Antrag: Art. 16 ist ersatzlos zu streichen

Zu Art. 26

Es fehlt eine Definition, ab wann von einer umfangreichen Bearbeitung von besonders schützenswerte Personendaten auszugehen ist.

Für die Möglichkeit zur Stellungnahme danken wir Ihnen bestens. Wir hoffen, dass unsere Argumente bei der weiteren Bearbeitung des Geschäfts Berücksichtigung finden und würden uns darüber freuen.

Mit freundlichen Grüssen

SCHWEIZERISCHE ZAHNÄRZTE-
GESELLSCHAFT SSO

Simon Gassmann, Rechtsanwalt LL.M.

Ivo Bühler, Rechtsanwalt

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Bundesamt für Justiz BJ
3003 Bern

Per Mail: jonas.amstutz@bj.admin.ch

Bern, 13. Oktober 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellung nehmen zu können. Der Schweizerische Städteverband vertritt die Städte, städtischen Gemeinden und Agglomerationen in der Schweiz und damit gut drei Viertel der Schweizer Bevölkerung.

1. Allgemeine Einschätzung

Der Städteverband ist mit der Stossrichtung der neuen Datenschutzgesetzgebung hin zu mehr Transparenz und Selbstbestimmungsrecht für die Nutzerinnen und Nutzer einverstanden. Unsere Mitgliedstädte begrüssen die Bestimmungen, die die Entwicklungen der technologischen Verhältnisse und des europäischen Rechts aufnehmen.

Für die Schweizer Wirtschaft ist die Sicherstellung der Kompatibilität mit dem europäischen Recht zentral. Hiesige Unternehmen, die in der EU tätig sind und eine nDSG/VDSG-konforme Datensicherheit gewährleisten, sollen davon ausgehen können, dass sie damit auch die Mindestanforderungen im EU-Raum erfüllen und umgekehrt. Die Schweiz soll weiterhin von der EU als Drittland mit angemessenem Datenschutz anerkannt werden, denn davon hängt die wirtschaftliche Position und die Wettbewerbsfähigkeit der Schweiz entscheidend ab. Ohne freien Datenfluss würden sich für Schweizer Unternehmen erhebliche Wettbewerbsnachteile ergeben.

Dabei müssen sich die administrativen Belastungen und die mit der Umsetzung der Datenschutzvorgaben verbundenen Kosten – insbesondere für KMUs – jedoch in einem vertretbaren Rahmen bewegen.

Der Städteverband ist zudem überzeugt, dass der sichere Umgang mit personenbezogenen Daten das Vertrauen der Bevölkerung in digitale Technologien stärkt. Ein verbesserter Datenschutz kann somit auch die fortschreitende Digitalisierung stärken.

Monbijoustrasse 8, Postfach, 3001 Bern
Telefon +41 31 356 32 32
info@staedteverband.ch, www.staedteverband.ch

2. Bemerkungen zu konkreten Artikeln

Trotz der grundsätzlichen Unterstützung sind aus dem Kreis unserer Mitglieder mehrere kritische Bemerkungen eingegangen, die wir Ihnen im Folgenden gerne zukommen lassen:

- Sorgfaltspflichten/Dokumentationspflichten: Im revidierten Datenschutzgesetz fehlen weitgehend Pflichten, Dokumentationen zu führen und aufzubewahren. Die Botschaft hielt fest, "anstelle einer allgemeinen Dokumentationspflicht wurde eine Bestimmung über ein Verzeichnis der Bearbeitungstätigkeiten eingefügt. Die Vernehmlassung hat ergeben, dass eine allgemeine Dokumentationspflicht zu wenig definiert ist". Der Gesetzgeber hatte demnach bewusst entschieden, bestimmte Dokumentationspflichten im Gesetz zu regeln und bei anderen darauf zu verzichten. Der vorliegende Entwurf der Verordnung sieht nun mehrere solche Pflichten vor (Art. 3 Abs. 4: Aufbewahrung von Systemlogs für zwei Jahre; Art. 18 Abs. 5: Aufbewahrung von Datenschutzfolgenabschätzungen für zwei Jahre; Art. 19 Abs. 5: Aufbewahrung der Dokumentation von Sicherheitsverletzungen für drei Jahre; Art. 20 Abs. 5: Aufbewahrung der Gründe für eine Einschränkung bei Betroffenenrechten für mindestens drei Jahre), die kumuliert von grosser Relevanz sind, und unseres Erachtens nach einer gesetzlichen Regelung rufen.

- Art. 3 Abs. 4, Zweckbindung der Verwendung von Systemlogs: Diese hätte auf formeller Gesetzesstufe verankert werden müssen. Sie widerspricht dem Zweckbindungsgrundsatz, der an die vom Verantwortlichen transparent gesetzten Zwecke anknüpft. Danach spricht nichts dagegen, dass ein Verantwortlicher die sog. Logs überwacht und evaluiert, z.B. zu Analysezwecken, wenn er dies ausdrücklich in der Datenschutzerklärung auch deklariert bzw. beschreibt.

- Art. 13, Modalitäten der Informationspflichten: In Art. 19 des revidierten Datenschutzgesetzes ist die Informationspflicht für den Verantwortlichen verankert, indessen nicht für den Auftragsbearbeiter. Zudem ist eine eigene Informationspflicht des Auftragsbearbeiters nicht logisch und widerspräche dessen Weisungsbindung.

- Art. 15 und 16, Information bei der Bekanntgabe von Personendaten und über die Berichtigung, Löschung usw.: Diese Informationspflicht hat keine Grundlage im revidierten Datenschutzgesetz, weder für Private noch für Bundesorgane, wäre in ihrer Umsetzung aber einschneidend. Eine solche Pflicht dürfte nicht auf Verordnungsstufe geregelt werden. Zudem wird hier wieder, wie in Art. 13, der Auftragsbearbeiter verpflichtet. Dabei müsste er Informationen bekanntgeben, die ihm gar nicht vorliegen.

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme. Zusätzlich verweisen wir Sie gerne auf die ausführliche Stellungnahme der Stadt Lausanne (im Anhang), die wir Ihnen direkt zustellen.

Freundliche Grüsse

Schweizerischer Städteverband

Präsident

Kurt Fluri, Nationalrat
Stadtpräsident Solothurn

Direktor

Martin Flügel

Stiftung für Konsumentenschutz
Nordring 4
Postfach
3001 Bern

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern
Per E-Mail:
jonas.amstutz@bj.admin.ch

Rückfragen:
Lucien Jucker, Leiter Datenschutz / Digitalisierung / IT
l.jucker@konsumentenschutz.ch

Bern, 30. September 2021

Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum BG über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Vielen Dank für die Möglichkeit, an der Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) teilzunehmen.
Die Stiftung für Konsumentenschutz ist eine Nichtregierungs-Organisation, die sich seit 1964 für die Rechte und Interessen von Konsumentinnen und Konsumenten einsetzt.

Der Konsumentenschutz nimmt zum Vorentwurf (VE-VDSG) wie folgt Stellung:

Die VE-VDSG folgt sprachlich dem Beispiel des neuen Datenschutzgesetzes (nDSG). Das ist leider kein Grund zur Freude. Dem Konsumentenschutz ist zwar absolut bewusst, dass das Datenschutzrecht technologieneutral und möglichst abstrakt formuliert werden muss. Dennoch weist das VE-VDSG zahlreiche schwammige Formulierungen auf, die letztendlich den Sinn der Regulierung untergraben und zu viel Interpretationsspielraum offenlassen.
Das sieht man an mehreren Stellen: In Art. 1 Abs. 2 VE-VDSG wird mitgeteilt, dass die Massnahmen «in angemessenen Abständen» überprüft werden sollen. Das macht in Bezug auf die unterschiedlichen Risikofaktoren zwar Sinn – dennoch sollte auch eine Periodizität festgelegt werden, also «in angemessenen, regelmässigen Abständen».
Besonders schwammig ist die in Artikel 2 VE-VDSG verwendete Formulierung «Soweit angemessen, müssen die Massnahmen […] folgende Schutzziele erreichen». Dieser Artikel gibt den Datenbearbeiterinnen und Datenbearbeitern durch die Formulierung «soweit angemessen» bereits einen grossen Ermessensspielraum. Dennoch relativiert der erläuternde Bericht auf Seite 17 zusätzlich die «Schutzziele», mit der Überlegung, dass nicht alle Schutzziele in allen Fällen relevant sind.

Somit wird sowohl für die Angemessenheit als auch für die Relevanz der Schutzziele auf das Ermessen der für die Datenbearbeitung verantwortlichen Person abgestellt. Dadurch entstehen also zwei grosse Ermessensspielräume. Diese erschweren das Beweisen eines Vorsatzes, der für eine strafbare Sorgfaltsverletzung nach Art. 63 nDSG notwendig ist. Kurzum: Die schwammige Sprache droht ein ohnehin eher schwaches Datenschutzgesetz weiter zu verwässern.
Damit diese Strafbestimmung nicht zahnlos wird, muss Artikel 2 VE-VDSG weiterhin «Schutzziele erreichen» und nicht wie teilweise gefordert «Schutzziele anstreben» lauten. Ausserdem soll sowohl die Formulierung «soweit angemessen» im VE-VDSG als auch die entsprechende Passage auf Seite 17 des erläuternden Berichts («Es ist durchaus vorstellbar, dass nicht jedes Schutzziel […] ») im erläuternden Bericht ersatzlos gestrichen werden.

Mit Art. 16 nDSG erhält neu der Bundesrat die Kompetenz zu entscheiden, in welche Länder Personendaten übertragen werden dürfen. Kriterien für die Entscheidung des Bundesrates fehlen im nDSG. Diese Kriterien sind in Art. 8 des VE-VDSG aufgelistet. Gemäss Art. 8 Abs. 6 VE-VDSG muss der EDÖB vor der Entscheidung des Bundesrats konsultiert werden. Damit diese Entscheidung nicht durch politische Überlegungen beeinflusst wird, soll der EDÖB weiterhin die zugrundeliegende Einschätzung vornehmen. Mindestens soll dem EDÖB ein Veto-Recht zukommen, damit er eine politisch motivierte, unsachliche Entscheidung verhindern kann. Die Entscheidungen, Anpassungen und Änderungen inkl. Begründungen müssen der Öffentlichkeit zugänglich gemacht werden.

Als positiv wertet der Konsumentenschutz, dass das Auskunftsrecht von Privatpersonen im VE-VDSG ein wenig gestärkt wird. Insbesondere begrüssen wir, dass die betroffene Person bei Verweigerungen, Einschränkungen und Aufschüben eines Auskunftsbegehrens innerhalb von 30 Tagen informiert werden und dieser Entscheid protokolliert werden muss.
Noch wichtiger ist die Regelung, dass die auskunftssuchende Person über die Höhe der ausnahmsweisen Beteiligung vorgängig informiert werden muss. Die Möglichkeit, daraufhin das Gesuch innert 10 Tagen zurückzuziehen ist eine willkommene Neuerung im VE-VDSG. Leider bleibt das Risiko bestehen, dass Datenbearbeiterinnen ohne sachliche Gründe eine Kostenbeteiligung verlangen – diese Kostenbeteiligung soll unserer Meinung nur für objektiv querulatorische Auskunftsbegehren gelten.
Ausserdem fehlt eine explizite Einwilligung in diese Kostenbeteiligung in diesem Entwurf – nach Ablauf von 10 Tagen können also max. 300 Franken für die Auskunft verrechnet werden. Besser wäre die Regelung, dass die auskunftssuchende Person aktiv in die Kostenbeteiligung einwilligen muss.
Letztlich ist es schade, dass die Verlängerung der Frist zur Auskunftserteilung auch im VE-VDSG ohne definierte Obergrenze möglich ist. Das Auskunftsbegehren ist für Konsumentinnen ein grundlegendes Instrument im Datenschutzgesetz – ohne Auskunft kann niemand wissen, welche Daten über einen bearbeitet werden. Die fehlende Maximaldauer ermöglicht eine willkürlich lange Bearbeitungsdauer der Auskunftsbegehren und untergräbt die Rechte der betroffenen Person.

Wir danken Ihnen für die Kenntnisnahme unserer Bedenken und stehen Ihnen bei Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Sig. Sara Stalder
Geschäftsleiterin

Sig. Lucien Jucker
Leiter Datenschutz

per Mail an:
jonas.amstutz@bj.admin.ch
Eidgen. Departement für Justiz EJPD
Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte I
3003 Bern

Zürich, 6. Oktober 2021
Wb/6540

VERNEHMLASSUNG
Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrter Herr Direktor
Sehr geehrte Damen und Herren

Wir beziehen uns auf den am 23. Juni 2021 veröffentlichen Entwurf zur totalrevidierten Verordnung zum DSG von 2020 (E-VDSG), zu dem wir uns gerne wie folgt vernehmen lassen.

Allgemeines

Die VDSG ist eine unselbständige Verordnung, was bedeutet, dass sie lediglich Ausführungsvorschriften zum DSG enthalten darf. Damit im Widerspruch stehen einige im E-VDSG enthaltene neue substanzielle Verpflichtungen der Verantwortlichen und Auftragsbearbeiter. Teilweise werden diese Verpflichtungen vorgeschlagen, obwohl sie vom Parlament explizit abgelehnt wurden. Eine derartige Missachtung des gesetzgeberischen Willens ist untragbar. Es handelt sich um folgende neue Verpflichtungen, die wegzulassen sind:

1. Art. 4: Bearbeitungsreglement
   Dieses stellt entgegen seiner systematischen Einordnung keine Massnahme der Datensicherheit dar und kann daher nicht auf Art. 8 Abs. 3 nDSG abgestützt werden.
2. Art. 13: Informationspflicht des Auftragsbearbeiters
   Diese Pflicht widerspricht Art. 19 Abs. 1 nDSG, nach dem sie nur die Verantwortlichen trifft.
3. Art. 15 und 16: Informationspflichten gegenüber Datenempfängern
   Beide Bestimmungen haben keine Grundlage im nDSG. Zudem wurde die Pflicht von Art. 16 vom Parlament explizit nicht aus dem E-DSG übernommen.

Genossenschaft der Urheber und Verleger von Musik
Coopérative des auteurs et éditeurs de musique
Cooperativa degli autori ed editori di musica

SUISA Bellariastrasse 82, Postfach 782, CH–8038 Zürich, Tel +41 44 485 66 66, Fax +41 44 482 43 33
www.suisa.ch, suisa@suisa.ch, MwSt.-Nr: CHE-105.838.471 MWST

4. Art. 18, 19 Abs. 5 und 20 Abs. 5: Dokumentations- und Aufbewahrungspflichten
   Derartige Pflichten benötigen eine Grundlage im Gesetz. Bereits in der Botschaft zum DSG wurde auf derartige Pflichten verzichtet; dem ist das Parlament gefolgt. Sie jetzt auf dem Verordnungsweg doch noch einzuführen, geht nicht an.

Zu einzelnen Bestimmungen

Art. 2 – Schutzziele der Massnahmen zur Datensicherheit

Art. 8 Abs. 3 nDSG spricht von «Mindestanforderungen» an die Datensicherheit, welche in der Verordnung zu erlassen sind. Vorgeschlagen werden in Art. 2 E-VDSG nun jedoch zu erreichende, umfangreiche sowie rigid und detailliert formulierte «Schutzziele», was nicht das gleiche ist. Vor dem Hintergrund der Strafbarkeit gemäss Art. 61 lit. c nDSG gehen sie viel zu weit. Sie sind deshalb zu streichen, oder zumindest ist zu statuieren, dass sie «anzustreben» (statt «zu erreichen») sind.

Art. 6 – Modalitäten der Datenbearbeitung durch Auftragsbearbeiter

Dass der Verantwortliche die vertrags- oder gesetzesgemässe Bearbeitung durch den Auftragsbearbeiter «sicherstellen» muss, impliziert eine Kausalhaftung. Das hat keine Grundlage im Gesetz und geht daher zu weit. Es kann lediglich verlangt werden, dass der Verantwortliche entsprechende angemessene und zumutbare Vorkehren trifft oder dazu Sorge trägt, dass Auftragsbearbeiter die Daten vertrags- und gesetzeskonform bearbeiten.

Art. 9 – Datenschutzklauseln und spezifische Garantien bei Auslandbekanntgabe

Die lit. j. und k. dehnen auf dem Verordnungsweg mittelbar verschiedene Verpflichtungen auf den Empfänger von Daten im Ausland aus. Eine solche Ausdehnung bedarf einer Grundlage in einem formellen Gesetz.
Lit. j. und k. Ziff. 1 widersprechen gar Art. 19 Abs. 4 bzw. 25 Abs. 1 nDSG. Denn diese beiden Gesetzesbestimmungen legen den Umfang der Informations- und der Auskunftspflicht abschliessend fest.
Im weiteren würde lit. k zu einer extraterritorialen Geltung von Schweizer Recht führen, was völkerrechtswidrig und von daher gar nicht durchsetzbar ist.
Schliesslich ist lit. j rein praktisch oft undurchführbar, weil der Datenempfänger im Ausland je nach erhaltenen Daten die betroffenen Personen und ihre Adressen nicht kennt, um sie zu informieren.
Beide Bestimmungen sind daher zu streichen.

Art. 13 – Modalitäten der Informationspflichten

Bei dieser Bestimmung sollte hinzugefügt werden, dass die Information auf einer Website des Verantwortlichen sowie das Anbringen der notwendigen Hinweise auf die Website in der Regel genügend sind, um den Informationspflichten nachzukommen. Eine solche Regelung erscheint heutzutage zumutbar.

Art. 19 – Meldung von Verletzungen der Datensicherheit

Unklar ist, in welchem Verhältnis Abs. 3 zu Art. 24 Abs. 4 nDSG steht. Danach ist die betroffene Person nur zu informieren, «wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.» Diese Einschränkung sollte ausdrücklich in die VDSG Eingang finden.

Art. 23 – Ausnahmen von der Kostenlosigkeit der Auskunft
Die in Abs. 2 festgelegte Kostenbeteiligung von maximal CHF 300 ist unrealistisch tief. Sie trägt dem Umstand keineswegs Rechnung, dass eine umfangreiche Recherche in grossen Unternehmen oder Konzernen rasch in die Zehntausende von Franken gehen kann. Eine so tiefe Limite ist vor allem auch im Hinblick auf den Schutz der Interessen der betroffenen Personen kontraproduktiv: Wenn die Kostenbeteiligung dem Missverhältnis der Interessen wie vom Gesetzgeber intendiert Rechnung tragen soll, kann sich der Verantwortliche viel eher auf das Missverhältnis berufen und eine Kostenbeteiligung verlangen. Deswegen ist die Limite entweder ganz zu streichen oder substanziell zu erhöhen.

Angemessen scheint hingegen, vom Verantwortlichen zu verlangen, dass, wenn er eine Kostenbeteiligung verlangt, deren Höhe dem Antragsteller bekanntgibt, bevor er das Auskunftsbegehren bearbeitet, damit der Antragsteller weiss, worauf er sich einlässt und er Gelegenheit hat, sein Auskunftsbegehren zurückzuziehen.

Wir danken Ihnen für die unseren Ausführungen entgegengebrachte Aufmerksamkeit und ersuchen Sie um wohlwollende Berücksichtigung unserer Anliegen.

Mit freundlichen Grüssen

SUISA

B. Wittweiler

Bernhard Wittweiler
RA Dr. iur., Abteilungsleiter Rechtsdienst

Sunrise UPC GmbH
Thurgauerstrasse 101B
8152 Glattpark (Opfikon)

Sunrise.net

Eidgenössisches Justiz-
und Polizeidepartement EJPD

CH-3003 Bern

Per Email an: Jonas.amstutz@bj.admin.ch

Opfikon, 14. Oktober 2021

Stellungnahme zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zu oben genanntem Geschäft Stellung beziehen zu können und nehmen diese gerne innerhalb der angesetzten Frist wahr.

Sunrise UPC GmbH ist der zweitgrösste Telekomanbieter in der Schweiz. Telekommunikationsdienstleistungen werden immer komplexer und hängen deshalb stark von hoch entwickelten technischen Infrastrukturen ab. Software- und Hardwaredefekte, menschliches Versagen, Viren und Hackerangriffe können die Service-Qualität sowie die in Bearbeitung stehenden Daten beeinträchtigen. Es ist daher von grosser Relevanz für unsere Geschäfts- und Privat-Kunden, Mitarbeiter sowie für uns als Unternehmen, dass hier zeitnah Klarheit in Bezug auf das neue Datenschutzgesetz und der dazugehörigen Verordnung herrscht. Dies insbesondere auch im Hinblick auf die Äquivalenz zu den Vorgaben der Europäischen Union, was aus wirtschaftlicher und politischer Sicht nicht zu unterschätzen ist.

1 Grundsätzliche Bemerkungen

Wir möchten den Zeitplan der Umsetzung nicht gefährden, jedoch trotzdem auf bestehende Unstimmigkeiten im vorliegenden Entwurf der VDSG hinweisen. Auf eine völlige Neuausarbeitung des Entwurfes ist aus zeitlichen Gründen zu verzichten, jedoch dürfen mit der Verordnung keine Vorgaben einfliessen, ohne dass eine gesetzliche Grundlage dafür vorhanden wäre. Die Verordnung ist darauf beschränkt, die gesetzlichen DSG-Vorgaben durch Detailvorschriften näher auszuführen und nicht neue gesetzliche Normen aufzunehmen. Des Weiteren besteht absolut kein Anlass, mit der Verordnung einen Swiss Finish zu unterstreichen. Dies verbessert unseres Erachtens den Nutzen für die Konsumentinnen und Konsumenten nicht und verlangt der Wirtschaft einen unnötig administrativen Mehraufwand ab.

2 Spezifische Anpassungen oder Streichungen

2.1 Bestimmungen betreffend die Bundesorgane

Da sich im Entwurf diverse Vorgaben für die Bundesorgane analog denjenigen für Privatpersonen verändern sollen, sind auch diese entsprechend anzupassen oder wo notwendig zu streichen. Aus diesem Grunde unterstützt Sunrise UPC als nicht Bundesorgan und Mitglied der asut vollumfänglich die Eingaben von Swico.

2.2 Bestimmungen betreffend die Privatpersonen

Als Mitglied der asut haben wir deren Eingabe entsprechend mitgestaltet. In diesem Sinne unterstützen wir die asut-Eingabe, welche sich auf diejenige der Swico abstützt. Die von der asut explizit aufgeführten Artikel 17-19, welche die Swico so nicht eingegeben hat, unterstützen auch wir von Sunrise UPC.

Wir danken ihnen bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Marcel Huber
Chief Corporate Affairs Officer

Luzern, 13.10.2021

Stellungnahme Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Vorbemerkung

Die Suva schliesst sich der Stellungnahme des Vereins Unternehmens-Datenschutz (VUD) an. Wie der VUD ist die Suva generell der Ansicht, dass bei zahlreichen Bestimmungen in der VDSG die gesetzliche Grundlage fehlt oder sie dem Willen des Gesetzgebers gar direkt widersprechen. Sie sind daher zu streichen. Zudem sollte auf zu detaillierte Bestimmungen verzichtet werden. Ebenfalls unterstützt die Suva die Forderung des VUD nach einer Übergangsfrist von einem Jahr für die Erstellung der Verzeichnisse und – falls darauf entgegen den Anträgen nicht verzichtet wird – auch für das Bearbeitungsreglement.

Bemerkungen und Anpassungsvorschläge

Artikel	Text	Bemerkung	Anpassungsvorschläge
1 Abs. 1	Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a. Zweck, Art, Umfang und Umstände der Datenbearbeitung; b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen; c. der Stand der Technik; d. Implementierungskosten.	Der Grundsatz, dass Verantwortliche und Auftragsbearbeiter eine dem Risiko angemessene Datensicherheit gewährleisten müssen, wird hier aufgegriffen (Art. 8 Abs. 1 revDSG). Zu Abs. 1: Massnahmen zur Datensicherheit sind nicht «angemessen», sondern «geeignet», wie dies Art. 8 Abs. 1 revDSG auch sagt. «Angemessen» kann nur das resultierende Sicherheitsniveau sein. Man sollte deshalb auch in Art. 1 Abs. 1 von «geeigneten» Massnahmen sprechen, um terminologische Widersprüche zu vermeiden. Zu lit. a): je höher der Schutzbedarf, desto höher sind auch die Anforderungen an die Massnahmen (z.B. bei besonders schützenswerten Personendaten, oder bei vollständig automatisierter Bearbeitung). Zu lit. b): die Anforderungen an die Massnahmen sind höher, wenn die Eintrittswahrscheinlichkeit höher ist. Zu lit. c): es geht dabei um die gegenwärtigen *und* bewährten Techniken, nicht um unerforschte Techniken. Zu lit. d): bei mehreren möglichen Massnahmen darf die kostengünstigste Option gewählt werden. Problematisch ist, dass der Bundesrat von der falschen Vorstellung ausgeht, dass Art. 8 revDSG, der hier konkretisiert	Statt von «angemessenen» Massnahmen ist von «geeigneten» Massnahmen zu sprechen. Zu schreiben ist: «b. die verbleibenden potenziellen Aus-wirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit (Restrisiko).» «Implementierungskosten» ist durch «Implementierungsaufwand» zu ersetzen.

Artikel	Text	Bemerkung	Anpassungsvorschläge
		wird, mehr als die Datensicherheit i.e.S. regelt (CIA). Es geht weder um Bearbeitungsgrundsätze noch Betroffenenrechte. Die Beispiele in den Erläuterungen sind teilweise falsch. Ob z.B. eine Bearbeitung durch eine KI oder einen Menschen erfolgt, ist für die Frage der Datensicherheit nicht relevant. Ferner ist der Begriff des «Risikos» (Bst. b) falsch formuliert. Zudem geht es hier nicht um das Bruttorisiko, sondern das Nettorisiko. Der Begriff «Implementierungskosten» impliziert, dass anderer Aufwand nicht relevant ist. Das ist falsch. Ebenso falsch ist die Ausführung in der Erläuterung, dass übermässige Kosten nicht Statt von «angemessenen» Massnahmen ist von «geeigneten» Massnahmen zu sprechen. Zu schreiben ist: «b. die verbleibenden potenziellen Aus-wirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit (Restrisiko).» «Implementierungskosten» ist durch «Implementierungsaufwand» zu ersetzen.	
1 Abs. 2	Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.	Ist die Gefährdung für die Rechte der Betroffenen grösser, so ist der Abstand der nächsten Prüfung kürzer. Die Formulierung «periodisch» wurde gestrichen. Die Prüfung muss ab einem gewissen Risiko standardisiert erfolgen (Pflicht zur Verwendung von ISO 27001?). Der Fokus auf die «angemessenen Abstände» ist zu eng. Wesentlich ist, dass sie in «angemessener Weise» überprüft werden. Der Begriff des «Abstands» impliziert nach wie vor eine Periodizität, die aber nicht zwingend ist, etwa wenn sich die Umstände nicht verändert haben.	Statt «angemessenen Abständen» ist «angemessener Weise» zu schreiben.
2	Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen: a. Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen.	Es muss nicht zwingend jedes dieser Schutzziele relevant sein, es muss aber begründet werden können, weshalb nicht. Zu lit. b: Der Begriff «Anlage» wurde ergänzt, es sind dabei auch mobile Bearbeitungsanlagen gemeint (z.B. Mobiltelefone oder Tablets). Zu lit. g: auch die Veränderung von Personendaten muss nachträglich überprüfbar sein.	Statt «erreichen» ist «anstreben» zu schreiben. Der Katalog der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden.

Artikel	Text	Bemerkung	Anpassungsvorschläge
	b. Zugangskontrolle: Der Zugang zu den Ein-richtungen und Anlagen, in denen Personen-daten bearbeitet werden, wird unbefugten Personen verwehrt. c. Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht. d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert. e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungs-systemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert. f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personen-daten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden. h. Bekanntgabekontrolle: Es kann überprüft werden, wem Personendaten mit Hilfe von Ein-richtungen zur Datenübertragung bekannt gegeben wurden. i. Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden. j. Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität). k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung	Zu lit. h: damit sollen auch die Empfänger der Daten identifiziert werden können (das Organ ist ausreichend). Lit. i, j und k wurden neu eingefügt. Zu lit. i: z.B. die Erstellung eines Backup-Konzepts. Zu lit. j: das System selbst soll automatisch darauf aufmerksam machen, dass eine Fehlfunktion vorliegt. Zu lit. k: der Verantwortliche oder Auftragsbearbeiter muss reaktive Massnahmen treffen zur Minderung der Folgen bei einer Verletzung der Datensicherheit. Die Verwendung des Worts «erreichen» impliziert, dass die Schutzziele vollständig erfüllt werden, was weder erforderlich noch möglich ist. Zu treffen sind nur angemessene Massnahmen; eine vollständige Sicherheit ist nicht erforderlich. Die aufgeführte Liste ist überdies veraltet, zu absolut und zu detailliert formuliert. Zudem geht es grundsätzlich um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. So ist es auch in Art. 32 Abs. 1 lit. b DSGVO definiert. Die Regelung zwingt zu einer Dokumentation für jede Datenbearbeitung (u.a. warum bestimmte der aufgeführten Schutzziele nicht relevant sind im konkreten Fall). Das widerspricht dem Willen des Gesetzgebers, der eine solche umfassende Dokumentationspflicht abgelehnt hat.	In diesem Fall wäre die Liste auch konform mit Art. 32 DSGVO.

Artikel	Text	Bemerkung	Anpassungsvorschläge
3 Abs. 1	Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.	Unternehmen müssen gemäss dem Wortlaut von Art. 3 Abs. 1 E-VDSG Datenbearbeitungen protokollieren, wenn sich aus der Datenschutz-Folgenabschätzung ergibt, dass trotz der ergriffenen Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht. Diese Bestimmung ist in mehrerlei Hinsicht problematisch und sollte ersatzlos gestrichen werden: *Erstens* fehlt ihr eine gesetzliche Grundlage. Es geht hier nicht primär um die Protokollierung zur Gewährleistung der Datensicherheit, sondern sie dient in erster Linie der *nachträglichen* Feststellung, ob es zu einer unbefugten Bearbeitung des Verantwortlichen bzw. seines Auftragsbearbeiters gekommen ist. Sollen unerlaubte Datenabflüsse, Malware, Einbrüche etc. entdeckt werden, sind andere Dinge zu protokollieren als die reguläre Nutzung der Daten (die Hacker und Malware vermeiden o-der löschen werden). Zur Feststellung einer Verletzung der Datensicherheit eignet sie also nicht und ist damit unverhältnismässig. Art. 8 revDSG, welcher als Grundlage der Bestimmung dient, behandelt nur die Datensicherheit i.e.S. Nur solche sollte der Bundesrat gemäss Art. 8 Abs. 3 revDSG ausführen (und nur die Verletzung solcher können auch zu einer Strafbarkeit führen). *Zweitens* ist das Ergebnis der DSFA kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. In der Re-gel wird eine DSFA nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenbearbeitung. Dies hat jedoch mit Datensicherheit nichts zu tun. Die Erläuterungen des E-VDSG bestätigen sogar, dass es (auch) um die Gewährleistung der zweckkonformen Bearbeitung geht. *Drittens* muss eine solche Bearbeitung kraft Art. 21 revDSG ohnehin dem EDÖB oder Datenschutzberater vorgelegt werden. Eben dies dient bereits dem Ziel, eine solche oder andere Massnahme vorzuschlagen, soweit die Bearbeitung überhaupt umgesetzt werden kann. Hier pauschal eine spezifische Massnahme ohne Berücksichtigung der Umstände vorzuschlage ist ein Schuss ins Blaue.	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung erreicht das Ziel materiell nicht und zielt an der Sache vorbei.

Artikel	Text	Bemerkung	Anpassungsvorschläge
		Viertens obliegt die Pflicht auch dem Auftragsbearbeiter, der jedoch die DSFA nicht kennen muss und eine solche schon gar nicht auszuführen hat. Massnahmen zur Datensicherheit obliegen zwar auch ihm, aber diese Protokollierung ist in ihrem Kern keine solche. Das erklärt den unlösbaren Widerspruch. Auch deshalb ist sie zu streichen. Unklar ist aufgrund der Norm, ob eine Protokollierungspflicht auch dann bestehen soll, wenn eine Datenschutz-Folgenabschätzung unterlassen wurde, obwohl sie nötig gewesen wäre. Dies wird aber wohl so sein.	
3 Abs. 2	Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.	Die Pflicht zur Protokollierung besteht unabhängig vom Risiko und muss daher bei jeder automatisierten Bearbeitung von Personendaten vorgenommen werden. Der Begriff der automatisierten Bearbeitung ist nicht definiert. Zu verstehen ist darunter aber das Gegenteil zur manuellen Bearbeitung – somit ist darunter eine elektronische oder vergleichbare Datenbearbeitung zu verstehen. Die Protokollierungen erscheinen als unverhältnismässig – ins-besondere, da auch das Lesen protokolliert werden muss. Auch im Falle von Bundesorganen ist die Regelung systematisch falsch und ohne gesetzliche Grundlage. Vgl. dazu die obigen Ausführungen.	Streichen (vgl. oben)
3 Abs. 3	Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.	Widerspruch zu den Mindestanforderungen an die Protokollierung gemäss den Absätzen 1 und 2. Abs. 3 bringt allerdings ebenfalls zum Ausdruck, dass es nicht um Verletzungen der Datensicherheit, sondern um etwaige unzulässige Bearbeitungen durch reguläre Benutzer geht. Diese stellen keine solche Verletzungen dar. Mit Empfänger ist die Organisation, nicht die Einzelperson gemeint.	Streichen (vgl. oben)
3 Abs. 4	Die Protokolle sind während zwei Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertrau-	Die Aufbewahrungsfrist von 2 Jahren muss eingehalten werden. Für eine solche Aufbewahrungspflicht gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet, abgesehen vom Verzeichnis.	Streichen. Es fehlt eine gesetzliche Grundlage. «getrennt vom System, in welchem die Personendaten bearbeitet wer-

Artikel	Text	Bemerkung	Anpassungsvorschläge
	lichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.	Die Regelung der getrennten Aufbewahrung ist technisch nicht ohne Weiteres oder nur mit erheblichem Aufwand umsetzbar. Protokolle werden dort erzeugt, wo sie anfallen – und nicht auf anderen Systemen. Ein Betrieb müsste somit von sämtlichen Protokollen Kopien anfertigen und sie manuell auf ein anderes System übertragen; der Aufbewahrungsort muss ein unabhängiges System sein. Dieser Vorgang birgt seinerseits Sicherheitsrisiken, abgesehen davon, dass der Aufwand enorm wäre Es würde genügen, wenn sichergestellt wird, dass die Protokolle ihrerseits sicher sind. Die Personen, welche die Verletzung von Datenschutzvorschriften verfolgen, erhalten gemäss Wortlaut keinen Zugang zu den Daten. Die Zweckbindung ist unzulässig, da sie strenger ist, als die Bearbeitungsgrundsätze dies erlauben. Damit fehlt der Regelung eine gesetzliche Grundlage. Ein Verantwortlicher oder Auftragsbearbeiter hat möglicherweise ein Interesse, die Logs auch aus anderen Gründen auszuwerten. Tut er dies DSG-konform, sollte dies auch möglich sein. Die Regelung ist insofern interessant, als heute viele Protokolle von IT-Systemen aus Gründen des Datenschutzes weniger lang aufbewahrt werden. Es kann mit Verweis auf den E-VDSG vertreten werden, dass eine Aufbewahrung von zwei Jahren ohne Weiteres verhältnismässig ist, wenn sogar der Gesetzgeber diese Frist standardmässig vorschreiben will. Korrekter-weise ist die Aufbewahrungsfrist aber als Mindestfrist auszugestalten. Gibt es Gründe, sie länger aufzubewahren, muss dies möglich sein.	den» ist zu streichen und durch «sicher» zu ersetzen. Die Regelung ist unverhältnismässig. aushebelt. Sofern eine Aufbewahrungsfrist überhaupt festgelegt wird, wo-für es keine Grundlage gibt, so macht eine starre Frist keinen Sinn und wäre unverhältnismässig. Sie muss von der Dauer der Datenbearbeitung abhängig und generell angemessen sein. Satz 2 ist zu streichen, da er dem DSG widerspricht, indem er die Bearbeitungsgrundsätze aushebelt. Ohnehin müsste der Personenkreis mit Zugang ist um jene erweitert werden, welche die Verletzung von Datenschutzvorschriften verfolgen.
4 Abs. 1	Bearbeitungsreglement von privaten Personen 1 Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie: a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen.	Die Pflicht, für Datenbearbeitungen mit einem hohen Risiko Bearbeitungsreglemente zu erstellen, besteht bereits nach der geltenden Verordnung. Allerdings wurde allgemein erwartet, auch aufgrund der Botschaft des Bundesrats und der parlamentarischen Beratung, dass die Bearbeitungsreglemente an-gesichts der neu eingeführten Dokumentations- und Informationspflichten (Verzeichnisse von Bearbeitungstätigkeiten, Datenschutz-Folgenabschätzungen, Datenschutzerklärungen) aus der Verordnung gestrichen werden. Das Bearbeitungsreglement dient augenscheinlich nicht der Sicherstellung der Datensicherheit i.e.S., sondern soll primär	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung ist unverhältnismässig und redundant. Es ist ein Swiss Finish.

Artikel	Text	Bemerkung	Anpassungsvorschläge
		die Einhaltung der Bearbeitungsgrundsätze und die weiteren Vor-gaben des Datenschutzes sicherstellen. Es fehlt der Bestimmung somit eine gesetzliche Grundlage, da Art. 8 revDSG nur Datensicherheit i.e.S. regelt. Der Vorgängernorm fehlt eben-falls die gesetzliche Grundlage, weshalb sie toter Buchstabe blieb bzw. bleiben musste (ihre Verletzung hat keine Rechtsfolgen). Demgegenüber steht der enorme Aufwand, den die Erstellung und Nachführung eines solchen Bearbeitungsreglements mit sich bringt. Wie bei Abs. 2 gezeigt wird, werden die wesentlichen Angaben ohnehin bereits im Rahmen der in solchen Fällen erforderlichen Datenschutz-Folgenabschätzung dokumentiert, der Rest im ohnehin zu erstellenden Inventar. Die Regelung ist somit überflüssig. Auch die DSGVO sieht eine solche Regelung nicht vor (Swiss Finish). Während ein «Profiling mit hohem Risiko» in der Praxis vermutlich kaum vorkommen wird, stellt sich die Frage, ab wann «umfangreich» besonders schützenswerte Personendaten bearbeitet werden. Dies dürfte mit Bezug auf die HR-Daten bei einem mittleren und grösseren Umfang bereits der Fall sein. Auch jedes Medienunternehmen wird erfasst sein, welches Be-richte über Politik und Gesellschaft enthält und damit auch besonders schützenswerte Personendaten (politische Ansichten etc.) bearbeitet. Es ist klar, dass besonders heikle Datenbearbeitungen eine betriebsinterne Regelung erfordern können. Dieser Aspekt ist jedoch über Art. 7 Abs. 1 revDSG bereits hinreichend geregelt. Der Erläuterungsbericht suggeriert, dass das Bearbeitungsreglement ein in sich geschlossenes Dokument sein muss. Dies ist praxisfremd und unnötig. Eine solche Pflicht zur «Urkunden-einheit» gilt auch sonst nirgends. Es besteht ferner das Risiko, dass Auskunftsersuchende über die Generalklausel versuchen werden, an das Bearbeitungsreglement heranzukommen.	

Artikel	Text	Bemerkung	Anpassungsvorschläge
		Die Dokumentationspflichten wurden aus der DSGVO übernommen und zusätzlich soll diese bestehende Pflicht nicht gestrichen werden. Dies führt zu einer erheblichen Erweiterung der Dokumentationspflichten.	
4 Abs. 2	Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. zur internen Organisation; e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.	Lit. a, b, c und f sind auch Bestandteile der Bearbeitungsverzeichnisse. Die übrigen Punkte müssen bei einer Datenschutz-Folgenabschätzung mitberücksichtigt werden, wenn diese für die Risiko-abwägung bzw. als Massnahme zur Reduktion der Risiken relevant sind, was in der Regel der Fall sein wird. Somit sind sie bereits dokumentiert. Die Liste zeigt im Übrigen, dass es augenscheinlich primär nicht um Datensicherheit, sondern die Einhaltung der Bearbeitungsgrundsätze und des restlichen Datenschutzgesetzes geht	Streichen (vgl. oben)
4 Abs. 3	Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.	Damit wird eine Pflicht zur Vorlage an den Datenschutzberater / die Datenschutzberaterin festgelegt, obwohl keine gesetzliche Verpflichtung besteht, diese Funktion überhaupt zu besetzen. Das Bearbeitungsreglement des Privaten muss weder publiziert noch dem EDÖB gemeldet werden.	Streichen (vgl. oben). In jedem Fall den zweiten Halbsatz streichen.
5 Abs. 1	Das verantwortliche Bundesorgan und dessen Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie: a. besonders schützenswerte Personendaten bearbeiten; b. ein Profiling durchführen;	Aufgrund der Auflistung muss praktisch für jede automatisierte Bearbeitung ein Reglement erstellt werden. Es ist unklar, warum die Bearbeitungsreglemente trotz Einführung der Verzeichnisse und der Datenschutz-Folgenabschätzung beibehalten werden.	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung ist unverhältnismässig.

Artikel	Text	Bemerkung	Anpassungsvorschläge
	c. Datenbearbeitungen im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG ausführen; d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen werden Personendaten zugänglich machen; e. Datenbestände miteinander verknüpfen; oder f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.	Zudem fehlt aus den zu Art. 4 E-VDSG erwähnten Gründen eine gesetzliche Grundlage. Vgl. im Übrigen die obigen Ausführungen zu Art. 4 E-VDSG. Zudem fehlt aus den zu Art. 4 E-VDSG erwähnten Gründen eine gesetzliche Grundlage.	
5 Abs. 2	Das Reglement muss mindestens die Angaben nach Artikel 4 Absatz 2 enthalten.	Die Formulierung ist unklar: Soll sie bedeuten, dass es allenfalls mehr Angaben enthalten muss?	Streichen (vgl. oben)
5 Abs. 3	Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutz-berater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen	Pflicht, das Bearbeitungsreglement dem Datenschutzberater und dem EDÖB bereitzustellen (auf Anfrage).	Streichen (vgl. oben)
6 Abs. 1	Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.	Der erste Satz wiederholt einerseits eine Banalität, ist anderer-seits aber ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall ein-geschränkt ist, auch dann, wenn ihm nichts vorgeworfen wer-den kann. Dem ist nicht so. Es ist ohnehin nicht klar, was «für den Datenschutz verantwortlich» meint. Strafrechtliche Verantwortlichkeit kann es nicht sein, und aufsichtsrechtliche Verantwortlichkeit setzt ebenfalls Kontrollmöglichkeiten voraus. Wird die Verantwortlichkeit schliesslich als zivilrechtliche Haftung verstanden, dann wird mit dieser Regelung eine vom Gesetz-geber nicht vorgesehene Kausalhaftung eingeführt. Hierfür fehlt eine gesetzliche Grundlage. Dies würde auch über Art. 82 Abs. 3 DSGVO hinausgehen. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR. Die Formulierung «sicherstellen» ist zudem inhaltlich falsch. Der Verantwortliche kann nur «dafür Sorge tragen». Auch der zweite Satz ist mangelhaft, da ihm ebenfalls eine gesetzliche Grundlage fehlt. Nach Art. 9 Abs. 1 Bst. a revDSG hat der Verantwortliche zu sorgen, dass die Daten so bearbeitet werden, wie er es selbst darf. Nach Satz 2 hat er jedoch auch für die Durchsetzung seines eigenen Vertrags zu sorgen, selbst wenn dieser strenger sein sollte als das Gesetz. Macht	Satz 1 streichen, da kein Mehrwert, jedoch verwirrend und falls als Kausalhaftung verstanden ohne gesetzliche Grundlage. Ohnehin ist «sicherstellen» durch «dafür Sorge tragen» zu ersetzen. Satz 2 streichen, da kein Mehrwert, jedoch verwirrend und ohne gesetzliche Grundlage, was die Pflicht zur Vertragsdurchsetzung betrifft.

Artikel	Text	Bemerkung	Anpassungsvorschläge
		er also einen zu strengen Vertrag, aber erlaubt er seinem Auftragsbearbeiter eine Bearbeitung, die noch dem Gesetz entspricht, ist diese Vorschrift bereits verletzt. Gemeint ist viel-leicht auch eine Bezugnahme auf Art. 9 Abs. 1 DSG («… Bearbeitung … kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden…»). Dies müsste in der Verordnung aber auch nicht wiederholt werden. Die Regel verwirrt also mehr als sie nutzt. Schon nach Art. 9 Abs. 1 Bst. a revDSG hat der Verantwortliche dafür zu sorgen, dass das DSG eingehalten wird. Das genügt.	
6 Abs. 2	Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.	Der Sinn und Zweck dieser Regelung erschliesst sich nicht, da der Regelungsgehalt bereits durch die Art. 16 und 17 revDSG (Bekanntgabe von Personendaten ins Ausland) gedeckt ist. Gemäss Erläuterungsbericht entspricht der neue Art. 6 Abs. 2 E-VDSG dem geltenden Art. 22 Abs. 3 VDSG. Dabei handelt es sich aber um eine Bestimmung für Bundesorgane, während Art. 6 Abs. 2 E-VDSG sowohl für Datenbearbeitungen Privater als auch für solche von Bundesorganen gelten soll. Aus dem Erläuterungsbericht geht nicht hervor, warum diese Bestimmung nun auch für Private gelten soll (oder warum es sie über-haupt braucht bzw. auf welche Rechtsgrundlage sie sich stützt). Die Regelung würde nur dort halbwegs Sinn machen, wo ein Schweizer Verantwortlicher einen ausländischen Auftragsbearbeiter bemüht Daten zu bearbeiten, ohne dass es zu einer Bekanntgabe aus der Schweiz kommt und somit Art. 16 revDSG nicht greift. Systematisch wäre aber auch dieser Fall in Art. 16 revDSG zu regeln und nicht in der VDSG. Es ist dies ein absoluter Sonderfall. Eine eigene Regelung in der VDSG rechtfecht-fertigt sich dadurch nicht. Die Regelung ergibt sich im übrigen sowieso bereits aus Art. 9 Abs. 1 Bst. a revDSG, und zwar systematisch korrekt, während sie hier systematisch falsch angelegt ist: Im Falle einer Auftragsbearbeitung geht es um die Sicherstellung eines gleichwertigen Datenschutzes, da der Auftragsbearbeiter die Daten gar nicht in eigener Regie bearbeiten darf. Es geht darum sicherzustellen, dass die Daten nur so bearbeitet werden, wie der Verantwortliche dies darf – und so steht es schon in Art. 9 Abs. 1 Bst. a revDSG.	Streichen. Die Regelung steht im Konflikt mit Art. 16 f. revDSG und Art. 9 Abs. 1 Bst. a revDSG, welche diesen Sachverhalt bereits ab-schliessend regeln.

Artikel	Text	Bemerkung	Anpassungsvorschläge
		Es ist allerdings zweifelhaft, ob die Autoren der Regelung diesen Sonderfall überhaupt im Blick hatten. Vermutlich wurde die Regel einfach übernommen, weil es sie schon gab.	
6 Abs. 3	Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich genehmigt hat.	Kern der Regelung ist, dass der Beizug von Unterauftragsbearbeitern im Falle von Bundesorganen *schriftlich* genehmigt wer-den muss. Das entspricht dem Standard der DSGVO; Art. 9 Abs. 3 revDSG sieht keine Schriftform vor. Hierbei handelt es sich um eine Umsetzung der EU Richtlinie 2016/680 (Justiz und Polizei). Diese verlangt in Art. 22 Abs. 2, dass im öffentlichen Sektor die Zustimmung schriftlich erteilt werden muss. Gemäss Botschaft des Bundesrates zu Art. 8 Abs. 3 E-DSG kann die vorgesehene Genehmigung sowohl im privaten als auch im öffentlich-rechtlichen Bereich spezifischer oder allgemeiner Art sein. Die Botschaft führt aus, dass im Falle einer allgemeinen Genehmigung zum Beizug von Subunternehmern, der Auftragsbearbeiter den Verantwortlichen über jede Änderung, wie den Wechsel oder den Beizug neuer Unterauftrags-bearbeiter, informieren muss, damit dieser bei Bedarf Ein-spruch erheben kann. Es ist somit zulässig, dass Behörden ihren Dienstleistern eine grundsätzliche Genehmigung erteilen, Subunternehmer beizuziehen, sofern bei allfälligen Änderungen eine Informationspflicht der Dienstleister besteht und die Behörde ein Vetorecht hat. Wird das Vetorecht ausgeübt, dann führt dies in der Regel bei Standarddienstleistungen zu einem Kündigungsrecht. Gemäss den Erläuterungen zum E-VDSG schliesst die schriftliche Form auch die elektronische Form mit ein. Damit entspricht die Formulierung von Art. 28 Abs. 2 DSGVO, welche ebenfalls «schriftlich» vorschreibt, damit aber auch den Fall des Nachweises durch Text meint. Es sollte ferner klargestellt werden, dass eine allgemeine Genehmigung (analog zur Regelung der DSGVO) zulässig ist, da es Bundesorganen sonst nicht möglich sein wird, Dienste von Standard-Online-Services zu beziehen. Diese verwenden ausschliesslich diese Methode.	Klarstellung, dass eine Genehmigung in Textform genügt und sie auch in allgemeiner Form erfolgen kann (beides analog DSGVO).

Artikel	Text	Bemerkung	Anpassungsvorschläge
7	Das Bundesorgan informiert die Datenschutz-beraterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvor-schriften entstehen.	Bundesorgane sind verpflichtet, eine Datenschutzberater*in zu bezeichnen (Art. 27 f DSG). Eine weitere Informationspflicht des Bundesorgans an die Datenschutzberater*in ist bereits in Art. 29 E-VDSG enthalten. Diese ist allgemeiner formuliert und umfasst grundsätzlich auch die Information über Auftragsbearbeitungen, sofern diese relevant sind. Die Formulierung der Norm ist zu salopp. Es ist nicht klar, was «Probleme» sind. Die Norm stellt aber klar, dass Art. 28 Abs. 2 lit. a E-VDSG die Datenschutzberater*in *nicht* verpflichtet ist, *jede* Datenbearbeitung zu prüfen; andernfalls wäre eine Information bei Auftragsbearbeitungsverträgen a priori nicht erforderlich.	Satz 2 ist zu streichen, da unnötig. Jedenfalls ist er präziser zu formulieren.
10 Abs. 1	Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.	Massnahmen sind angemessen, wenn sie dem Stand der Technik sowie den konkreten Umständen entsprechen. Die An-forderungen an die Massnahmen sind höher, wenn es sich beispielsweise um besonders schützenswerte Personendaten handelt. Wiederum kann der Exporteur nicht «sicherstellen», sondern nur dafür Sorge tragen. Der Erläuterungsbericht verlangt fälschlicherweise, dass der Empfänger verpflichtet werden muss, das Schweizer Datenschutzrecht einzuhalten. Das ist falsch. Einhalten muss er nur den Vertrag. Die Vorschrift führt zu einer Kausalhaftung und ist in der Praxis nicht zu erfüllen. Nicht einmal das Bankenrecht kennt eine der-art strenge Regelung. Zudem verlangen die aktuellen Standardvertragsklauseln, die in der Praxis flächendeckend eingesetzt werden, ohnehin entsprechende Sorgfaltspflichten des Exporteurs.	Der Begriff «sicherstellen» ist durch «in angemessener Weise Sorge zu tragen» zu ersetzen.
12 Abs. 2	Der Verhaltenskodex enthält mindestens die Angaben nach Artikel 9 Absatz 1 und muss vorgängig vom EDÖB genehmigt werden.	Dies wird nicht möglich sein, da der Verhaltenskodex naturgemäss abstrakt und nicht für spezifische Unternehmen formuliert ist. Er wird somit beispielsweise die «Empfänger» (nicht: «Kategorien von Empfängern») nicht nennen. Dies ist jedoch gemäss dieser Bestimmung erforderlich.	Der Verhaltenskodex «muss mindestens jene Punkte regeln, die nach dem Sinn und Zweck von Art. 9 Absatz 1 zu Regeln sind.»

Artikel	Text	Bemerkung	Anpassungsvorschläge
		Ferner sollte nicht von «Angaben» die Rede sein, sondern von «Regelungen» oder «Punkten».	
13 Abs. 1	Der Verantwortliche und der Auftragsbearbeiter teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit.	Art. 13 Abs. 1 E-VDSG verweist auf eine Informationspflicht des Auftragsbearbeiters, was im Erläuterungsbericht auch nochmals ausdrücklich betont wird. Das revDSG sieht aber keine Informationspflicht des Auftragsbearbeiters vor, diese besteht gemäss Art. 19 revDSG (korrekterweise) nur für den Verantwortlichen. Da das Gesetz keine solche Pflicht für den Auftragsbearbeiter vorsieht, kann sie auch nicht über die Verordnung eingeführt werden. Art. 19 revDSG verlangt eine Information der betroffenen Personen, nicht eine Mitteilung. Für eine Information der betroffenen Person genügt ein Zugänglichmachen. Dies entspricht auch dem Verständnis unter der DSGVO. Es sollte durch die Wortwahl «mitteilen» keine Verschärfung impliziert werden. Stattdessen sollte analog zu den Informationspflichten im Finanzmarktrecht der Begriff «zur Verfügung stellen» verwendet werden. Das bringt auch besser zum Ausdruck, dass die Information ein Betroffenenrecht darstellt, dessen Ausübung eine gewisse Mitwirkung des Betroffenen verlangt. Die Erläuterungen erwähnen, dass eine Kommunikation über eine Website nicht immer genügt. Die Person müsse wissen, dass sie die Informationen auf einer bestimmten Website findet, und es wird z.B. für Telefongespräche nahegelegt, dass ihr der Link mündlich mitgeteilt wird. Solche Ausführungen sind praxisfremd. Es sollte stattdessen festgehalten werden, dass die Information auf der Website genügt. Das entspricht der heutigen Praxis. Alles andere ist praxisfremd. Auch die Ausführungen in den Erläuterungen, wonach die betroffene Person die wichtigsten Informationen stets auf der ersten Kommunikationsstufe erhalten muss, ist schlicht falsch. Es gibt hierfür keine gesetzliche Grundlage, und es lässt jede Selbstverantwortung ausser Acht. Das ist auch deshalb bedenklich, weil der betroffenen Personen im Datenschutz eine Schlüsselrolle zukommt und es kontraproduktiv ist, ihr jede Ei-geninitiative abzunehmen.	Die Erwähnung des Auftrags-bearbeiters ist zu streichen. Es fehlt die gesetzliche Grund-lage. Seine Erwähnung macht auch keinen Sinn. Es sollte nicht das Wort «mit-teilen» verwendet werden, da es dafür keine gesetzliche Grundlage gibt. Korrekt wäre «Der Verantwortliche stellt die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form zur Verfügung.» Es sollte festgehalten werden, dass eine Information über eine Website in der Regel genügt.

Artikel	Text	Bemerkung	Anpassungsvorschläge
13 Abs. 2	Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.	Werden Piktogramme verwendet, müssen diese maschinenlesbar sein. Letzteres soll gemäss dem Erläuterungsbericht einen Vergleich verschiedener Dokumente und allgemein eine gewisse Automatisierung ermöglichen – es stellt sich die Frage, inwieweit dies ein Ziel des Datenschutzes ist. Die Pflicht unterliegt auch einem Überlegungsfehler. Die Piktogramme haben den Zweck, den Menschen einfacher als über Text anzusprechen und ihm zu ermöglichen, intuitiv auf eine Datenschutzerklärung zu reagieren. Soll dagegen eine automatisierte Auswertung einer Datenschutzerklärung erfolgen, müsste die Datenschutzerklärung selbst, nicht die Piktogramme maschinenlesbar bzw. ihre Inhalte entsprechend codiert sein, und zwar unabhängig davon, wie sie optisch dargestellt ist. Bei der Maschinelesbarkeit geht es ja gerade *nicht* um die optische Darstellung. Abgesehen davon gibt es für eine solche Pflicht keine gesetzliche Grundlage. Die Verwendung von Piktogrammen ist freiwillig, und daher darf der Verwender auch entscheiden, ob sie maschinenlesbar sind oder nicht, was auch immer dies bedeutet. Schliesslich fehlt es auch an Standards für solche Angaben. Ohne Standards macht eine solche Regel keinen Sinn.	Streichen. Es fehlt eine gesetzliche Grundlage. Die Regel macht auch keinen Sinn und führt im schlimmsten Fall zur Strafbarkeit. Dies kann wiederum dazu führen, dass keine Piktogramme verwendet wer-den.
14	Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin.	Dies betrifft insbesondere die Statistik und Forschung. Die Regelung ist jedoch praxisfremd, denn es kann auch aus den Umständen hervorgehen, dass eine Auskunft freiwillig ist (Beispiel: Kundenzufriedenheitsumfrage eines Krankenversicherers)	Ergänzen mit «soweit dies nicht aus den Umständen er-sichtlich ist»
15	Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.	Für diese «Informationspflicht bei der Bekanntgabe von Personendaten» gibt es keine gesetzliche Grundlage. Sie ist auch nach EU-Recht, auf welches sich der Erläuterungsbericht beruft, für private Datenbearbeiter nicht vorgeschrieben. Gegenüber der bisherigen Regelung in der VDSG wird die Vollständigkeit neu hinzugefügt, d.h. die Daten dürfen nicht lückenhaft sein. Die Regelung ist praxisfremd. Sie lässt sich nicht vernünftig umsetzen. Soll fortan jede E-Mail an eine andere Organisation einen entsprechenden Hinweis enthalten? Dazu kommt, dass	Streichen, jedenfalls für private Datenbearbeiter. Es gibt keine gesetzliche Grundlage. Swiss Finish. Sie ist in dieser Form nicht praktikabel.

Artikel	Text	Bemerkung	Anpassungsvorschläge
		der Empfänger ohnehin selbst verpflichtet ist, die Bearbeitungsgrundsätze einzuhalten und angemessene Massnahmen zu treffen, sich über die Richtigkeit der Daten zu vergewissern. Eine Information durch die übermittelnde Person unterläuft dies bzw. verabsolutiert eine der möglichen Vergewisserungsmass-nahmen. Dies widerspricht dem Gesetz. Hinzu kommt, dass ein Auftragsbearbeiter etwas bekanntgeben soll, das er womöglich gar nicht hat.	
16	Der Verantwortliche informiert die Empfängerinnen und Empfänger, denen er Personendaten bekanntgegeben hat, unverzüglich über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten, ausser die Benachrichtigung ist unmöglich oder mit einem unverhältnismässigen Aufwand verbunden.	Die in Art. 16 E-VDSG vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren, war bereits im Entwurf des revDSG vorgesehen und wurde vom Parlament gestrichen. Die Einführung dieser Pflicht über die revidierte Verordnung würde daher dem Willen des Parlaments widersprechen. Dieselbe Bestimmung verweist zu-dem auf ein Recht auf Einschränkung der Bearbeitung von Personendaten, das so im revDSG nicht besteht. Die Regelung erwähnt zudem die «Einschränkung» der Bearbeitung. Dies spielt auf Art. 18 DSGVO an, welche Bestimmung in der Schweiz so nicht existiert.	Streichen. Es gibt keine gesetzliche Grundlage
18	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.	Schriftlich ist an dieser Stelle mit Papierform oder elektronischer Form gemeint. Der Begriff ist nicht als handschriftlich zu verstehen. Für eine solche Aufbewahrungspflicht gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet, abgesehen vom Verzeichnis. Die Regelung geht ferner davon aus, dass eine Datenschutz-Folgenabschätzung nie erneuert wird. Dies entspricht jedoch nicht der Praxis. Es ist nicht klar, wie mit mehreren Datenschutz-Folgenabschätzungen umzugehen ist.	Klarstellen: «… muss in der aktuellsten Fassung während zwei Jahren …» Die Aufbewahrungspflicht ist zu streichen. Es fehlt eine gesetzliche Grundlage. So oder so ist sie als Mindestfrist auszugestalten. Es ist klarzustellen, dass Schriftlich «in Textform» meint.
19 Abs. 1	Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit: a. die Art der Verletzung; b. soweit möglich den Zeitpunkt und die Dauer; c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten; d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;	Art. 19 stellt eine Präzisierung von Art. 24 revDSG dar und ist so zu verstehen, dass im Falle einer Meldung an den EDÖB diese die in Art. 19 Abs. 1 VDSG aufgeführten Punkte enthalten muss. Die Einschränkung «soweit möglich» macht Sinn, da die Angabe in der Praxis oft nicht möglich ist.	Im Einleitungssatz ist aufzunehmen: «… bei einer melde-pflichtigen Verletzung …» Bst. e ist umzuformulieren: «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht»

Artikel	Text	Bemerkung	Anpassungsvorschläge
	e. die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen; f. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder die Folgen zu mildern; g. den Namen und die Kontaktdaten einer Ansprechperson.	Bst. a und b gehen über die DSGVO hinaus, doch dürfte dies in der Praxis kein Problem darstellen ausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem «Risiko» entspricht). Falsch formuliert ist hingegen Bst. e. Die «allfälligen Risiken» beinhalten bereits die Folgen für die betroffenen Personen. Richtig müsste es heissen «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht». Auch in Bst. f müsste nicht von den «Folgen», sondern vom «Risiko» die Rede sein. Gemildert werden kann entweder das Schadensausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem «Risiko» entspricht). Gemäss den Erläuterungen wird das in Art. 24 Abs. 2 revDSG erwähnte «voraussichtlich» so interpretiert, dass auch dann gemeldet werden muss, wenn das Vorliegen eines «hohen Risikos» nicht ausgeschlossen werden kann. Diese Aussage hilft nicht weiter, da es sich um einen Pleonasmus handelt. Der Be-griff «Risiko» beinhaltet bereits eine Wahrscheinlichkeits-über-legung, d.h. wie wahrscheinlich es ist, dass ein Schaden ein-tritt. Es bleibt dabei: Die Wahrscheinlichkeit muss eine gewisse Höhe aufweisen. Wünschenswert wäre schliesslich eine «de minimis»-Regelung, die jene Fälle ausschliesst, in welchen der EDÖB ohnehin nicht wirklich etwas tun kann oder will, obwohl ein hohes Risiko vorliegt (z.B. eine problematische E-Mail geht an den falschen Empfänger und ein Missbrauch durch diesen ist möglich). Damit können auch die Ressourcen des EDÖB geschont werden, die er für andere, für den Datenschutz wich-tigere Angelegenheiten einsetzen kann. Gemäss den Erläuterungen wird das in Art. 24 Abs. 2 revDSG erwähnte «voraussichtlich» so interpretiert, dass auch dann gemeldet werden muss, wenn das Vorliegen eines «hohen Risikos» nicht ausgeschlossen werden kann. Der Begriff «Risiko» beinhaltet bereits eine Wahrscheinlichkeitsüberlegung. Es bleibt dabei: Die Wahrscheinlichkeit muss eine gewisse Höhe aufweisen. Wünschenswert wäre schliesslich eine «de minimis»-Regelung, die jene Fälle ausschliesst, in welchen der EDÖB ohnehin nichts tun kann oder will, obwohl ein hohes Risiko vorliegt (z.B. eine problematische E-Mail geht an den falschen Empfänger und ein Missbrauch durch diesen ist	Es sollte eine «de minimis»-Regelung vorgesehen werden, in welchen trotz eines hohen Risikos für eine betroffene Person nicht gemeldet werden muss. Bst. f. sollte angepasst werden: "gegebenenfalls welche Mass-nahmen getroffen wurden …"

Artikel	Text	Bemerkung	Anpassungsvorschläge
		möglich). Damit können auch die Ressourcen des EDÖB geschont werden, die er für andere, für den Datenschutz wichtigere Angelegenheiten einsetzen kann.	
19 Abs. 2	Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.	Der Hinweis «bei Entdeckung der Verletzung der Datensicherheit» erscheint wenig sinnvoll. Zu diesem Zeitpunkt wird der Verantwortliche nie über alle Informationen verfügen, da sich diese immer erst über Zeit herausstellen. Der Hinweis kann ersatzlos gestrichen werden.	Streichung von «bei Entdeckung der Verletzung der Datensicherheit»
19 Abs. 5	Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.	Eine Dokumentationspflicht kennt zwar die DSGVO. Das revDSG sieht sie jedoch nicht vor. Daher kann sie und die entsprechende Aufbewahrungspflicht auch nicht auf dem Weg der Verordnung eingeführt werden. Noch die Botschaft zum revDSG hielt fest, dass keine allgemeine Dokumentationspflicht eingeführt werden soll. Genau dies wird hier (und in anderen Bestimmungen) durch die Hintertür versucht. Es bleibt jedenfalls unklar, wozu die Dokumentations- und Aufbewahrungspflicht dient, ausser allenfalls dem EDÖB. Da sich aus der Systematik aber ergibt, dass ohnehin nur meldepflichtige Verletzungen zu dokumentieren sind, erschliesst sich auch dieser Sinn nicht wirklich: Ist gemeldet und interessiert sich der EDÖB dafür, wird er sofort nachfragen. Tut er dies nicht, wird er kaum später darauf zurückkommen. Der Hinweis auf alle «zusammenhängenden Tatsachen» ist falsch, denn er suggeriert, dass Tatsachen nur für die Dokumentationspflicht erforscht werden müssen, was sicherlich nicht erforderlich ist. Warum hier drei statt wie sonst zwei Jahre vorgesehen sind, ist unklar.	Streichen. Es fehlt die gesetzliche Grundlage. Die Norm ist auch nicht nötig. Der Begriff «Tatsachen» ist durch «und dokumentierten Tatsachen» zu präzisieren.
20 Abs. 3	Die Auskunft muss für die betroffene Person verständlich sein.	Sie muss verständlich sein. Ob die betroffene Person sie im konkreten Fall versteht, ist nicht relevant. Beim Auskunftsbegehren geht es darum, die bearbeiteten Daten mitzuteilen. Müssen diese noch so erläutert werden, dass sie für die betroffene Person verständlich sind, kann dies zu einem unverhältnismässigen Aufwand führen. Das Auskunftsrecht bietet Zugang zu Daten, nicht ein Recht darauf, die Da-	Den Begriff «für die betroffene Person» streichen. Statt «verständlich» soll «im Grundsatz nachvollziehbar sein, sofern damit kein unverhältnismässiger Aufwand verbunden ist» verwendet werden. Eine Alternative wäre folgende

Artikel	Text	Bemerkung	Anpassungsvorschläge
		tenbearbeitung so lange erklärt zu bekommen, bis sie die jeweilige Person versteht. Eine solche Pflicht hat keine Grundlage im Gesetz. Beispielsweise können die im Rahmen einer klinischen Studie bearbeiteten Daten oder technische Logdaten für die betroffene Person unverständlich sein. Müssen diese zuerst so dargestellt werden, dass sie für die betroffene Person verständlich sind, sind aufwändige Erläuterungen erforderlich, mit-unter auch sehr viel Fachwissen. Abgesehen davon, dass dies nicht unbedingt innerhalb von 30 Tagen erfolgen kann, sprengt dies jeden Rahmen und ist unverhältnismässig. Nirgends in Europa wird das Auskunftsrecht so verstanden.	Formulierung: «Die Auskunft darf nicht irreführend sein.»
20 Abs. 4	Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.	Es fehlt eine gesetzliche Grundlage für eine echte Verpflichtung der betroffenen Person. Insofern macht Satz 2 wenig Sinn. Lässt sich die Identität der betroffenen Person nicht verifizieren, erhält sie auch keine Auskunft.	Begriff «Identifizierung» ersetzen durch den Begriff «Authentifizierung»
20 Abs. 5	Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.	Diese Dokumentation kann bspw. durch eine Kopie des Antwortschreibens erreicht werden. Bei einer mündlichen Auskunft müsste daher z.B. eine Telefonnotiz erstellt werden. Das revDSG sieht keine solche Dokumentations- und Aufbewahrungspflicht vor. Sie kann nicht auf dem Verordnungsweg eingeführt werden. Sie ist auch wenig sinnvoll. Sie zwingt den Verantwortlichen, Personendaten entsprechend länger aufzubewahren bzw. mehr Personendaten zu beantworten, als er dies womöglich tun würde. Die betroffene Person erhält eine Antwort auf ihr Ersuchen. Will sie dagegen vorgehen, kann sie diese Antwort ins Recht legen. Die Bestimmung sorgt nur für zusätzlichen Aufwand. Wie sich die drei Jahre herleiten, ist unklar.	Streichen. Es fehlt eine gesetzliche Grundlage. Die Bestimmung bietet keinen Mehrwert, sorgt aber für zusätzlichen Auf-wand.
21 Abs. 1	Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.	Das DSG nimmt auf den Begriff der gemeinsamen Verantwortlichen sonst normalerweise keinen Bezug. Die Regelung ist je-doch konsequent. Unklar ist, welche Rechtsfolge die «Unzuständigkeit» eines Verantwortlich hat.	Es ist zu präzisieren: "Sind für die Bearbeitung von Personen-daten mehrere gemeinsam ver-antwortlich …"

Artikel	Text	Bemerkung	Anpassungsvorschläge
21 Abs. 2	Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen.	Diese Bestimmung ist verwirrlich, da sie impliziert, dass der Auftragsbearbeiter selbst eine Auskunftspflicht hat, wenn er faktisch in der Lage sein sollte, eine Auskunft zu erteilen bzw. er das Auskunftsgesuch in einem solchen Fall nicht weiterleiten muss, auch wenn er es nicht beantwortet. Das kann nicht sein. Die Regelung sollte präzisiert werden.	Am Ende sollte es heissen: «sofern er das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet.»
22 Abs. 1	Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen.	Die Frist kann erst dann zu laufen beginnen, wenn das Begehren klar und die betroffene Person korrekt identifiziert ist. Dies ist sie zu Beginn häufig nicht.	Zu präzisieren: «… seit dem Vorliegen eines klaren Begehrens und der korrekten Identifikation der betroffenen Person.»
23 Abs. 2	Die Beteiligung beträgt maximal 300 Franken.	Der Betrag wird nicht verändert, weil es seit seiner Einführung zu keiner relevanten Teuerung gekommen sei und der Betrag nicht abschreckend sein soll. Allerdings steht dieser Kostendeckel im Vergleich zum Aufwand, den ein Auskunftsersuchen trotz entsprechender Strukturen mit sich bringen kann, in keinem Verhältnis (z.B. können umfassende Schwärzungen erforderlich sein, was Kosten pro Fall von CHF 10'000 mit sich bringen kann). Auch die DSGVO kennt keine betragsmässige Begrenzung, sondern verlangt, dass er «angemessen» ist. Auch im Öffentlichkeitsrecht kann eine Gebühr verlangt werden. Der Betrag soll durchaus abschreckend sein, weil er die betroffenen Personen dahingehend diszipliniert, Auskunftsersuchen nur dann zu stellen, wenn sie wirklich angezeigt sind und nicht aus Jux.	Betrag den Verhältnissen an-passen (mindestens CHF 3’000) Alternativ ist die Bestimmung zu streichen, da die angemessene Kostenbeteiligung bereits in Abs. 1 enthalten ist. Beispiel: Aufwand bis CHF 500 trägt das Unternehmen, dar-über hinaus müssen die Kosten zu 50% übernommen werden. ist.
23 Abs. 3	Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen.	Es ist zu präzisieren, dass die Antwortfrist von 30 Tagen erst danach beginnt.	Präzisieren: «Erst danach beginnt die Frist zur Beantwortung des Auskunftsbegehrens.»
25	Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen muss folgende Aufgaben wahrnehmen: a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden. b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft	Es ist schon konzeptionell nicht richtig, dass der Datenschutzberater die Aufgaben «wahrnehmen» muss, er muss sie «haben». Zu lit. a: Die breite der Prüfpflicht geht am Ziel vorbei, als sie impliziert, dass der Datenschutzberater im Grund kein Berater mehr ist, sondern als "Datenschutzpolizist" agieren sollte, d.h. alles und jeden in Bezug auf den Datenschutz zu überprüfen. Richtig wäre stattdessen, dass seine beratende Funktion betont wird, und zwar dort, wo ihn die verantwortlichen	Die Bestimmung sollte gestrichen werden, da im Gesetz bereits alles nötig gesagt wird. Sie stammt noch aus einer Zeit, in welcher das Gesetz noch keine solchen Ausführungen enthielt. Wird sie beibehalten, ist sie zu präzisieren: «Der Datenschutz-beraterin oder dem Datenschutzberater eines

Artikel	Text	Bemerkung	Anpassungsvorschläge
	diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG ab-sehen will.	Stellen beiziehen wollen. Das ist auch das Prinzip, das der Gesetzgeber bei der DSFA verfolgt: Wenn der Verantwortliche die DSFA nicht dem EDÖB vorlegen will, was er kann, dann kann er sie stattdessen dem Berater vorlegen. So sieht es auch Art. 10 Abs. 2 Bst. a revDSG vor. Dem ist hier Rechnung zu tragen. Der Berater sollte nur auf Beizug aktiv werden. Abgesehen davon ist beim bestehenden Vorschlag unklar, in welchem Umfang die Bearbeitungen zu prüfen sind (alle, einige, nur die ihm vorgelegten, nur nach Risiko) und welche Folgen es hat, wenn der Datenschutzberater dieser Aufgabe nicht nachkommt. Die Erläuterungen implizieren, dass alle Bearbeitungsaktivitäten überprüft werden müssen, was nicht richtig sein kann. Auch hier kann risikoorientiert geprüft werden. Mit den «Voraussetzungen» sind die internen Datenschutzvorschriften gemeint, die der Datenschutzberater ebenfalls über-prüfen soll. Die Erläuterungen implizieren daher, dass der Datenschutzberater eine andere Stelle sein soll als die interne Datenschutzstelle, welche solche Vorschriften ausarbeitet. Dies ist dem Konzept des Datenschutzbeauftragten der DSGVO angelehnt. Die Erläuterungen betonen auch, dass der Datenschutzberater für die Datenbearbeitung nicht verantwortlich ist. Zu lit. b: Nur das Vorlegen der DSFA dem/der DSB genügt nicht, der/die DBS muss bei der Erstellung der DSFA mitwirken. Dabei müssen die Risikobewertung und vorgeschlagenen Massnahmen geprüft werden.	privaten Verantwortlichen müssen folgende Aufgaben übertragen worden sein:» Bst. a ist anzupassen: "Wo sie oder er beigezogen wird, prüft sie oder er die Bearbeitung …"
26	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.	Unternehmen mit weniger als 250 Mitarbeitenden (wohl nicht FTE) müssen folglich nur diejenigen Bearbeitungstätigkeiten in Verzeichnissen dokumentieren, die die genannten Kriterien er-füllen, d.h. eine Datenbearbeitung durchführen, die ein hohes Risiko mit sich bringt. Unklar ist, ab wann «umfangreich» besonders schützenswerte Personendaten bearbeitet werden. Genügt die Bearbeitung von HR-Daten? Sind die Voraussetzungen für die Befreiung nicht erfüllt, ist das Verzeichnis für alle Bearbeitungsaktivitäten zu führen. Dies impliziert jedenfalls der Wortlaut der Bestimmung. Art. 12 Abs. 5 revDSG erlaubt die Ausnahme nur, wenn ein «geringes Risiko» vorliegt. Demnach ist der Bundesrat der Auf-	Es ist klarzustellen, dass wenn eine der beiden Voraussetzungen erfüllt ist, die Verzeichnis-pflicht nur für die entsprechen-den Bearbeitungen mit hohem Risiko gelten. Der Begriff der Mitarbeitenden ist durch "Vollzeitstellen" zu er-setzen. Es ist eine Übergangsfrist zur Umsetzung der Verzeichnis-pflicht von einem Jahr vorzusehen.

Artikel	Text	Bemerkung	Anpassungsvorschläge
		fassung, dass wenn weder Bst. a noch b erfüllt ist, per se ein geringes Risiko vorliegt. Das würde den Anwendungsbereich von Art. 22 revDSG (DSFA) stark einschränken. Zudem ist darauf hinzuweisen, dass diese Ausnahme bei Art. 3 und 4 nicht vorgesehen ist, was zu absurden Folgen führt. Generell sollten für Verzeichnisse Übergangsfristen vorgesehen werden, da sie einen sehr hohen Aufwand mit sich bringen.	
31	Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von Personendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden.	Es ist unklar, was «sogleich» bedeuten soll. Es muss genügen, dass die Erfordernisse des Datenschutzes im Projekt rechtzeitig berücksichtigt werden.	Der Begriff «sogleich» ist durch «rechtzeitig» zu ersetzen.
32 Abs. 1	Das verantwortliche Bundesorgan meldet dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung. Der EDÖB nimmt diese Meldung in das Register der Bearbeitungstätigkeiten auf.	Bereits geplante automatisierte Bearbeitungstätigkeiten müssen gemeldet werden, was zu einem erheblichen Mehraufwand für die Dokumentation führt. Zudem muss jede geplante automatisierte Bearbeitung gemeldet werden, nicht nur solche mit einem (potenziellen) hohen Risiko. Die Meldung muss im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung erfolgen. Diese erfolgen oft auf der Basis eines vorgegebenen Rahmens, während die konkreten Entscheidungen erst im Verlauf des Projekts getroffen werden. Daraus folgt, dass die verlangten Angaben in dem Zeitpunkt in der Regel noch nicht in der genügenden Detailtiefe vorliegen werden. Zudem sollte sich gemäss Botschaft zu Art. 11 Abs. 4 E-DSG (Art. 12 Abs. 4 revDSG) keine Änderung im Vergleich zum bestehenden Recht ergeben. Eine Pflicht, geplante Datensammlungen dem EDÖB zu melden, besteht aber nach geltendem Recht nicht. Es fehlt daher an einer gesetzlichen Grundlage. Gemäss Erläuterungsbericht dient die frühe Meldung zudem nicht dem Persönlichkeitsschutz, sondern der Ressourcenplanung des EDÖB.	Streichen, es fehlt die gesetzliche Grundlage. Zudem liegen die zu melden-den Informationen im Zeit-punkt, in dem die Meldung er-folgen soll, in der Regel nicht in der genügenden Detailtiefe vor. Die Ressourcenplanung des EDÖB rechtfertigt zudem nicht den mit dieser frühen Meldung einhergehenden Mehraufwand der Bundesbehörden.

Artikel	Text	Bemerkung	Anpassungsvorschläge
		Art. 47 E-VDSG enthält eine Übergansbestimmung für automatisierte Bearbeitungstätigkeiten, die bei Inkrafttreten des E-VDSG bereits produktiv sind.	

ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern
Per E-Mail an: jonas.amstutz@bj.admin.ch

Zürich, 13. Oktober 2021

Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG). Das Versicherungsgeschäft ist von der Revision des Datenschutzrechts direkt betroffen. Für den Schweizerischen Versicherungsverband SVV ist deshalb die Revision dieser Verordnung von zentraler Bedeutung:

- Der Umgang mit Kundendaten bildet eine unentbehrliche Grundlage des Versicherungsgeschäfts. Versicherer sind auf die Daten ihrer Kundinnen und Kunden angewiesen und die Kunden darauf, dass Versicherer ihre Daten bearbeiten: Dies gilt beim Abschluss eines Versicherungsvertrags, während des Vertrags und im Schaden- bzw. Leistungsfall sowie für Aktivitäten im Bereich des Marketings.
- Zudem sind Mitgliedgesellschaften des SVV im Sozialversicherungsbereich an der Durchführung von obligatorischen Versicherungen beteiligt.

Gerne nehmen wir deshalb die Gelegenheit wahr, zur E-VDSG Stellung zu nehmen:

- Zu beachten gilt, dass die Versicherungsbranche in doppelter Hinsicht von der Vorlage betroffen ist, da für die Assekuranz sowohl die Vorgaben der E-VDSG für die Privatwirtschaft als auch die Vorgaben der E-VDSG für die Bundesorgane Geltung haben. Wie eingangs erwähnt, sind Mitgliedgesellschaften des SVV im Sozialversicherungsbereich an der Durchführung von obligatorischen Versicherungen beteiligt. Wir würden es daher begrüssen, wenn in der Verordnung eine Differenzierung innerhalb der Bundesorgane vorgenommen würde (soweit dies auf dieser Normstufe möglich ist). So machen gewisse Bestimmungen für Bundesorgane im Strafrechtsbereich Sinn, nicht jedoch für Bundesorgane im Sozialversicherungsbereich (siehe z.B. die pauschale Protokollierungspflicht für Bundesorgane gemäss Art. 3 Abs. 2 E-VDSG für alle automatisierten Datenbearbeitungen, die der SVV für den Sozialversicherungsbereich ablehnt).
- Ein weiterer grundsätzlicher Punkt betrifft die Inkraftsetzung des neuen Rechts: Die Totalrevision des Datenschutzrechtsrechts bringt markante Änderungen und zahlreiche neue Verpflichtungen für die Unternehmen mit sich. Dies verlangt nach einer angemessenen Umsetzungsfrist. Zumal im neuen DSG keine Übergangsfristen vorgesehen sind und das neue Recht (totalrevidiertes DSG samt totalrevidiertem Verordnungsrecht) bei dessen Inkrafttreten bereits vollständig implementiert sein muss. Dies sollte bei der Festlegung des Inkraftsetzungstermins berücksichtigt werden. Für die Umsetzungsarbeiten in den Unternehmen

Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14 – Postfach – CH-8022 Zürich – Zentrale +41 44 208 28 28 – svv.ch
Franziska Streich – franziska.streich@svv.ch – Direktwahl +41 44 208 28 63

ASA | SVV

erachten wir einen Zeitraum von mindestens einem Jahr, laufend ab Feststehen/Veröffentlichung der definitiven Fassung der Verordnung, als notwendig.

Für diese und weitere zentrale Anliegen der Assekuranz erlauben wir uns, Ihnen unsere Änderungsvorschläge und Überlegungen in der beiliegenden Unterlage zukommen zu lassen. Aufgrund der vielen von uns als notwendig erachteten Anpassungen lehnen wir den vorliegenden Verordnungsentwurf klar ab (siehe die beiliegende Unterlage mit den Anpassungsvorschlägen des SVV). Abschliessend verweisen wir auch auf die Stellungnahme von economiesuisse, welche sich ebenfalls ablehnend äussert und deren Haltung wir teilen.

Wir danken Ihnen für die Berücksichtigung unserer Vorschläge bei der weiteren Behandlung der Vorlage. Gerne stehen wir Ihnen für Rückfragen zur Verfügung.

Freundliche Grüsse
Schweizerischer Versicherungsverband SVV

Sandra Kurmann
Leiterin Bereich Finanz und Regulierung

Franziska Streich
Fachverantwortliche Recht

Stellungnahme SVV zur Totalrevision der Verordnung zum DSG (E-VDSG) **Beilage**

Die prioritären Anträge des SVV sind in der nachstehenden Tabelle **blau** gekennzeichnet.

E-VDSG	Anträge SVV	Begründung
Art. 2 Bst. b	**Ändern** b. Zugangskontrolle: Der Zugang zu den Einrichtungen ~~und Anlagen~~, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt.	• Gemäss dem erläuternden Bericht soll mit dem Begriff «Anlagen» zum Ausdruck kommen, dass auch der Zugang zu mobilen Bearbeitungsanlagen zu unterbinden ist. Dazu gehören gemäss erläuterndem Bericht beispielsweise Mobiltelefone oder Tablets (siehe erläuternder Bericht, Seite 18). • Eine Zugangskontrolle zu Mobiltelefonen oder Tablets ist nicht umsetzbar. Hier muss die Zugriffskontrolle gemäss Art. 2 Bst. a E-VDSG ausreichen. Wichtig ist, dass sich keine unberechtigten Personen Zugriff auf mobile Geräte verschaffen können. Siehe beispielsweise die Homeofficepflicht infolge Covid-19: Nicht jeder Mitarbeitende verfügt über eine eigene Wohnung, wo der Zugang zu mobilen Geräten kontrolliert erfolgen kann.
Art. 2 Bst. c, d und g	**Ändern** c. Datenträgerkontrolle: Das ~~Lesen, Kopieren, Verändern, Verschieben~~ Bearbeiten von Personendaten auf dem Datenträger oder das Entfernen von Datenträgern wird unbefugten Personen verunmöglicht. d. Speicherkontrolle: Unbefugte ~~Eingabe in den~~ Bearbeiten der Personendaten im Datenspeicher ~~sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten~~ wird verhindert.	• Anstelle einer Aufzählung der Bearbeitungsschritte schlagen wir vor, den Oberbegriff des Bearbeitens zu verwenden. Mit dem Begriff des Bearbeitens werden sämtliche Möglichkeiten abgedeckt. Der Begriff ist auch deckungsgleich mit dem neuen DSG (siehe Art. 2 und 5). • Es ist nicht klar, ob sich das Bearbeiten auf den Datenträger bezieht oder auf die darin enthaltenen Daten. Es sollte zwischen dem Bearbeiten des Datenträgers und den darin enthaltenen Daten differenziert werden. • Es ist nicht klar, was der Unterschied zwischen Datenträger (Bst. c) und Datenspeicher (Bst. d) ist.

E-VDSG	Anträge SVV	Begründung
	g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person ~~eingegeben oder verändert~~ bearbeitet wurden.	
Art. 3 Abs. 1	**Ändern** [1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, ~~Lesen,~~ Bekanntgeben, Löschen oder Vernichten.	• Auf die Protokollierung des «Lesen», da kaum umsetzbar, ist zu verzichten.
Art. 3 Abs. 2	**Streichen**	• Mitgliedgesellschaften des SVV sind im Sozialversicherungsbereich an der Durchführung von obligatorischen Versicherungen als Bundesorgane beteiligt. • Eine pauschale Protokollierungspflicht der Bundesorgane für alle automatisierten Bearbeitungen von Personendaten lehnen wir ab. Es fehlt hierfür eine Rechtfertigung bzw. im erläuternden Bericht (Seite 20) wird auf Art. 25 der EU-Richtlinie 2016/680 verwiesen. Sollte wegen dieser EU-Bestimmung aus Äquivalenzgründen eine einschlägige Regelung auf Verordnungsstufe notwendig sein, ist diese auf den Strafrechtsbereich zu limitieren. • Für den Nicht-Strafrechtsbereich, z.B. den Sozialversicherungsbereich, sollte Absatz 1 zur Anwendung kommen.

E-VDSG	Anträge SVV	Begründung
Art. 3 **Abs. 4**	**Ändern** [4] Die Protokolle sind während einem ~~zwei~~ Jahren ~~getrennt vom System, in welchem die Personendaten bearbeitet werden,~~ aufzubewahren und vor nachträglicher Veränderung zu schützen. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.	• Es ist die geltende Aufbewahrungsfrist von einem Jahr beizubehalten (siehe Art. 10 Abs. 2 VDSG). • Die Begründung, wonach Cyber-Angreifer in der Regel länger in einem System aufhalten, ohne erkennbaren Schaden anzurichten, ist nicht stichhaltig für eine Erhöhung der Aufbewahrungsfrist. Wenn ein Angreifer nur beobachtet, ohne Veränderungen vorzunehmen, dann sieht man das nicht und schafft mit einer Verlängerung der Aufbewahrungsfrist nur einen Mehraufwand. Die Herausforderung dabei ist, die gesammelten Protokolldaten sinnvoll auszuwerten. Eine Auswertungslösung, wie beispielsweise Splunk, erfordert bei einer grösseren Datenmenge eine Erweiterung der Lizenz, was mit hohen zusätzlichen Kosten verbunden ist, ohne dass dadurch ein höheres Schutzniveau erreicht wird. • Nicht zielführend ist auch das Erfordernis einer getrennten Aufbewahrung, da sich ein Angreifer auch in getrennten Systemen gleichzeitig bewegen kann. Zielführender wäre eine Vorgabe, wonach die Protokolle vor nachträglicher Veränderung zu schützen sind. Im Übrigen kann mit der Protokollierung alleine wohl kaum ein Cyberangriff aufgedeckt werden. Es braucht dafür eine Korrelation über verschiedene Systeme hinweg, angefangen beim Client, mit dem die Benutzer arbeiten, über Server und Datenbanken, auf die sie zugreifen, bis hin zu Netzwerkaktivitäten, welche dann in der Korrelation als Anomalie entdeckt werden können.
Art. 4	**Streichen**	• Für das in Art. 4 E-VDSG vorgesehene Bearbeitungsreglement für private Personen fehlt eine gesetzliche Grundlage. Wichtiges wie Pflichten gehören ins Gesetz (Art. 164 Bundesverfassung). Eine solche zusätzliche Pflicht hätte im Gesetz selber geregelt werden müssen. • Es genügt das Führen eines Verzeichnisses der Bearbeitungstätigkeiten, wie dies der Gesetzgeber in Art. 12 neues DSG statuiert.

E-VDSG	Anträge SVV	Begründung
		• Art. 4 E-VDSG führt zu einem grossen und unnötigen Dokumentationsaufwand, da Angaben doppelt (im Bearbeitungsreglement und im Bearbeitungsverzeichnis) geführt werden müssten. • Ein Mehrwert des Bearbeitungsreglements im Sinne der Transparenz ist nicht ersichtlich. Zumal mit dem Verzeichnis der Bearbeitungstätigkeiten ein Instrument geschaffen wurde, welches das Reglement ersetzt und im Falle von Bundesorgangen ebenfalls dem EDOEB gemeldet werden muss. Es ist unverständlich, warum das Reglement nun über die Verordnung durch die Hintertüre eingeführt werden soll, vor allem, wenn gewisse Angaben sich sogar aus dem Verzeichnis «kopiert» werden soll, was jedoch kaum so einfach umsetzbar sein wird. • Die technischen und organisatorischen Massnahmen sind Pflichten des Verantwortlichen, wie auch die Protokollierung der Zugriffsberechtigungen und der Zugriffe, womit sich eine Publikation erübrigt. Im Gegenteil wird sogar ein Risiko für die Verantwortlichen geschaffen, wenn betroffene Personen versuchen, über das Auskunftsbegehren Einsicht in das Reglement zu erhalten. • Weitere Angaben im Reglement müssen über die Informationspflichten ohnehin erfüllt werden. Mit einem Bearbeitungsreglement wird nur ein zusätzlicher administrativer Aufwand geschaffen, der keinen zusätzlichen Nutzen für die betroffenen Personen bringt. • Aus diesen Gründen ist auf ein zusätzliches Bearbeitungsreglement zu verzichten.
Art. 5	**Streichen**	• Siehe Begründung unter Artikel 4. • Konsequenterweise sollte bei einer Streichung von Art. 5 auch Art. 84b KVG bei einer künftigen Revision des KVG entsprechend angepasst werden.
Art. 6 Abs. 1	**Ändern**	• Der Verantwortliche kann nicht sicherstellen, sondern bloss für die vertrags- und gesetzesgemäss Bearbeitung sorgen (lassen).

E-VDSG	Anträge SVV	Begründung
	[1] Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er ~~muss sicherstellen~~ sorgt dafür, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.	• Unklar ist, warum «auftragsgemäss» gemäss geltendem Art. 22 VDSG durch «vertrags- oder gesetzesgemäss» ersetzt werden soll.
Art. 6 Abs. 2		• Wir gehen davon aus, dass in Bezug auf Art. 6 Abs. 2 E-VDSG die Länderliste im Anhang 1 der revidierten VDSG Anwendung findet.
Art. 6 Abs. 3	**Ändern** [3] Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich oder in einer anderen Form, die den Nachweis durch Text ermöglicht, genehmigt hat oder nicht innert angemessener Frist widerspricht.	• Im Zuge der fortschreitenden Digitalisierung sollte neben der Schriftform (Erfordernis der eigenhändigen Unterschrift gemäss OR) alternativ auch Textform möglich sein (siehe z.B. revidiertes VVG, das per 1. Januar 2022 in Kraft tritt und neu grossmehrheitlich die Textform alternativ neben der Schriftform vorsieht). • Zudem sollte anstelle einer Genehmigung alternativ auch ein Widerspruchsvorbehalt möglich sein.
Art. 7	**Streichen**	• Eine zusätzliche Informationspflicht des Bundesorgans an dessen Datenschutzberater/-in ist nicht notwendig, da der Datenschutzberater/-in bei der Anwendung des Datenschutzrechts gemäss neuem DSG mitwirkt. • Bundesorgane bzw. im Sozialversicherungsbereich tätige Versicherer verfügen über zahlreiche Verträge, welche eine Auftragsdatenbearbeitung beinhalten. Diesbezüglich ist ein risikobasierter Ansatz zu wählen. Der Datenschutzberater/-in kennt aufgrund des Verzeichnisses der Bearbeitungstätigkeiten die risikobehafteten Bearbeitungen. Eine zusätzliche Informationspflicht des Bundesorgans an dessen Datenschutzberater/-in, wie in Art. 7 vorgesehen, schafft keinen Mehrwert für die betroffenen Personen und ist nicht notwendig.

E-VDSG	Anträge SVV	Begründung
Art. 9 Abs. 1 Bst. j	**Streichen**	• Es ist nicht Aufgabe des Auftragsverarbeiters, die betroffenen Personen zu informieren. Dies ist Aufgabe des Verantwortlichen.
Art. 13 Abs. 1	**Ändern** [1] Der Verantwortliche ~~und der Auftragsbearbeiter~~ teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit, wobei ein Verweis auf eine Datenschutzerklärung auf der Website oder auf allgemeine Geschäftsbedingungen ausreichend ist.	• Eine Informationspflicht des Auftragsbearbeiters ist nicht praktikabel und unnötig. Der Auftragsbearbeiter erledigt seine Aufgaben nach Weisung und ausschliesslich nach dem vom Verantwortlichen vorgegebenen Zweck. Es gibt keinen Anlass, eine Informationspflicht des Auftragsbearbeiters auf Stufe Verordnung einzuführen. Hierfür gibt es auch keine gesetzliche Grundlage. • Im Interesse der Rechtssicherheit ist klarzustellen, wie der Informationspflicht nachgekommen werden kann. Der Verweis auf eine Website oder auf allgemeine Geschäftsbedingungen muss in der heutigen Zeit genügen.
Art. 13 Abs. 2	**Streichen**	• Diese Bestimmung ist in der vorgesehenen Formulierung unpraktikabel. • Es ist auch unklar, was maschinenlesbar bedeutet.
Art. 14	**Ändern** Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin~~.~~, sofern dies aus den Umständen nicht ersichtlich ist.	• Die Freiwilligkeit kann auch aus den Umständen ersichtlich sein, so dass ein Hinweis nicht notwendig ist.
Art. 15	**Streichen**	• Art. 15 E-VDSG statuiert zusätzliche Informationspflichten. Für diese Zusatzpflichten fehlt eine gesetzliche Grundlage im neuen DSG. • Diese Pflicht scheint zudem nicht umsetzbar/nicht praktikabel.

E-VDSG	Anträge SVV	Begründung
		• Letztlich ist es Sache der Unternehmen, die Einhaltung der Datenschutzgrundsätze sicherzustellen. Bei gesetzlich vorgesehenen Datenbearbeitungen ist die Information ohnehin unnötig.
Art. 16	**Streichen**	• Diese Pflicht war ursprünglich in Art. 19 Bst. b Vorentwurf DSG enthalten, wurde dann aber gestrichen. • Sie kann entsprechend dem Verfassungsgrundsatz, wonach Wichtiges wie Pflichten ins Gesetz gehören (Art. 164 Bundesverfassung), nun nicht auf Stufe Verordnung wieder eingeführt werden.
Art. 18	**Ändern** Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in einer anderen Form, die den Nachweis durch Text ermöglicht, festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.	• Siehe auch Ausführungen unter Art. 6 Abs. 3. • Schriftlichkeit ist weder erforderlich noch zeitgemäss (Digitalisierung). Neben der Schriftform (Erfordernis eigenhändiger Unterschrift gemäss OR) muss alternativ auch Textform möglich sein (siehe z.B. revidiertes VVG, das per 1. Januar 2022 in Kraft tritt und neu grossmehrheitlich die Textform alternativ neben der Schriftform vorsieht).
Art. 19 **Abs. 5**	**Ändern** 5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens ~~drei~~ ein Jahr~~e~~ aufzubewahren.	• Im E-VDSG finden sich unterschiedliche Aufbewahrungsfristen. Das ist umständlich, prozessual mühsam und wenig zweckmässig. • Eine einheitliche Aufbewahrungsfrist von einem Jahr erscheint angemessen.
Art. 20 **Abs. 3**	**Ändern** 3 Die Auskunft muss ~~für die betroffene Person~~ in einer Landessprache oder Englisch und verständlich verfasst sein.	• Sofern sich die Verständlichkeit auf die Sprache bezieht, so ist diese Anforderung auf die Landessprachen und Englisch zu begrenzen. Ansonsten müsste in jeder Sprache Auskunft gegeben werden.

E-VDSG	Anträge SVV	Begründung
Art. 20 **Abs. 4**	**Ändern** [4] Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken, ansonsten kann die Auskunft verweigert werden.	• In Art. 20 Abs. 4 E-VDSG ist festzuhalten, dass bei fehlender Mitwirkung der betroffenen Person, die Auskunft verweigert werden kann.
Art. 20 **Abs. 5**	**Ändern** [5] Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens ~~drei~~ ein Jahr~~e~~ lang aufzubewahren.	• Siehe Ausführungen zum Art. 19 E-VDSG.
Art. 23 **Abs. 1**	**Ändern** [1] Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. Weiter können bei mutwilligen und wiederholt unbegründeten Anfragen Kosten auferlegt werden.	• Mit einer Kostenauferlegung könnten Mehrfachanfragen oder querulatorische Anfragen reduziert werden.
Art. 23 **Abs. 2**	**Ändern** [2] Die Beteiligung beträgt maximal 300 Franken.	• Die Kostenbeteiligung sollte den Umständen Rechnung tragen. Eine Fixierung auf max. 300 Franken ist nicht sachgerecht. Die max. Beteiligung ist angemessen zu erhöhen.

E-VDSG	Anträge SVV	Begründung
Art. 25 Abs. 1 Bst. a	**Ändern** a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden.	• Art. 25 Abs. 1 Bst. a E-VDSG ist entsprechend zu ändern, wonach der Datenschutzberater/-in nicht jede Bearbeitung prüfen muss. Es sollte ein risikobasierter Ansatz gelten.
Art. 25 Abs. 1 Bst. b	**Ändern** b. Sie oder er ~~wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und~~ überprüft ~~diese~~ eine Datenschutz-Folgenabschätzung, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.	• Es muss den Unternehmen überlassen werden, wie die Prozesse bei einer Datenschutz-Folgenabschätzung unternehmensintern organisiert werden. Wichtig ist lediglich, dass der Datenschutzberater/-in eine Überprüfung vornimmt (wie dies in Art. 25 Abs. 1 Bst. b E-VDSG vorgesehen ist).
Art. 29 Abs. 2	**Ändern** [2] Es veröffentlicht die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters ~~im Internet und teilt diese~~ dem EDÖB ~~mit~~. Die Kontaktmöglichkeit zur Datenschutzberaterin oder zum Datenschutzberater muss im Internet geteilt werden.	• Der Name des Datenschutzberaters/-in sollte im Internet nicht veröffentlicht werden müssen. Es sollte einfach die Kontaktmöglichkeit zum Datenschutzberater im Internet ersichtlich sein.
Art. 31	**Streichen**	• Die Ernennung eines Datenschutzberaters/-in sollte auch für Bundesorgane freiwillig sein und ein entsprechender Anreiz geschaffen werden, dass eine Ernennung erfolgt. Anreiz könnte sein, dass z.B. eine Meldung der Bearbeitungsverzeichnisse unterbleiben kann. • Eine Informationspflicht der Bundesorgane gegenüber ihren Datenschutzberatern/-in bei Projekten zur automatisierten Datenbearbeitung wird abgelehnt. Diese Zusatzpflicht bringt keinen

E-VDSG	Anträge SVV	Begründung
		Mehrwert für die betroffenen Personen und führt zu einem unnötigen administrativen Aufwand für die Bundesorgane. Hierfür fehlt auch eine gesetzliche Grundlage.
Art. 32	**Streichen**	• Bundesorgane müssen nach Art. 12 Abs. 4 neuem DSG die Verzeichnisse ihrer Bearbeitungstätigkeiten dem EDÖB melden. Eine zusätzliche Pflicht zur Meldung jeder geplanten automatisierten Datenbearbeitung bringt keinen Mehrwert für die betroffenen Personen, führt zu einem unnötigen administrativen Aufwand für die Bundesorgane und zu einer Aufblähung des staatlichen Apparates (siehe auch begrenzte personelle Ressourcen des EDÖB, der alle diese Meldungen sichten müsste). • Siehe auch Ausführungen unter Art. 31 E-VDSG.
Art. 36	**Streichen** Werden Personendaten zu nicht personenbezogenen Zwecken, insbesondere Forschung, Planung und Statistik, und gleichzeitig zu einem anderen Zweck bearbeitet, so sind die Ausnahmen nach Artikel 39 Absatz 2 DSG nur für die Bearbeitung zu den nicht personenbezogenen Zwecken anwendbar.	• Es genügt Art. 39 des neuen DSG. Eine diesbezügliche Verordnungsbestimmung ist nicht notwendig. • Art. 36 E-VDSG stiftet nur Verwirrung und dient damit nicht der Rechtssicherheit.
Art. 43		• Hinweis: vgl. zu Art. 32. Im Falle einer Streichung von Art. 32 ist Art. 43 entsprechend anzupassen.
Art. 47		• Hinweis: vgl. zu Art. 32. Im Falle einer Streichung von Art. 32 ist auch Art. 47 zu streichen.
Art. 48	**Umsetzungsfrist von mindestens einem Jahr zwischen Verabschiedung der Endfassung der Verordnung durch den Bundesrat und dem Inkraftsetzungstermin**	• Die Totalrevision des Datenschutzrechtsrechts bringt markante Änderungen und zahlreiche neue Verpflichtungen für die Unternehmen mit sich. Die Umsetzung des neuen Rechts stellt eine hochkomplexe und äusserst zeitaufwendige Arbeit dar.

E-VDSG	Anträge SVV	Begründung
		• Das neue Recht verlangt unter anderem umfangreiche Anpassungen bei den Prozessen. Diese müssen zwischen den Geschäftsbereichen sauber koordiniert und in den IT-Systemen der Unternehmen abgebildet werden. Bei Prozess-/IT-Änderungen sind zudem angemessene Testzeiträume einzuplanen, um sicherzustellen, dass diese mit Inkraftsetzung des neuen Rechts zuverlässig live gehen können. Weiter sind zum Beispiel Kundendokumente/-unterlagen und Schulungsprogrammen und -materialien für die Mitarbeitenden zu überprüfen und anzupassen und Mitarbeiterschulungen durchzuführen. • Dies verlangt nach einer angemessenen Umsetzungsfrist. Zumal im neuen DSG keine Übergangsfristen vorgesehen sind und das neue Recht (totalrevidiertes DSG samt totalrevidiertem Verordnungsrecht) bei dessen Inkrafttreten bereits vollständig implementiert sein muss. • Für die Umsetzung des neuen Rechts muss die Veröffentlichung der Endfassung der Verordnung abgewartet werden. • Dies ist bei der Festlegung des Inkraftsetzungstermins zu berücksichtigen. Für die Umsetzungsarbeiten in den Unternehmen erachten wir einen Zeitraum von mindestens einem Jahr, laufend ab Feststehen/Veröffentlichung der definitiven Fassung der Verordnung, als notwendig.

Swico
Lagerstrasse 33
CH-8004 Zürich

Tel. +41 44 446 90 90
www.swico.ch
info@swico.ch

Frau Bundesrätin Karin Keller-Sutter
Eidgenössiches Justiz- und Polizeidepartement EJPD

Ausschliesslich per Mail an:
Jonas.amstutz@bj.admin.ch

Zürich, 14. Oktober 2021

Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese gerne innerhalb der angesetzten Frist wahr.

Swico ist der Wirtschaftsverband der Digitalisierer und vertritt die Interessen etablierter Unternehmen sowie auch Start-ups in Politik, Wirtschaft und Gesellschaft. Swico zählt über 650 Mitglieder aus der ICT- und Online-Branche. Diese Unternehmen beschäftigen 56'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 40 Milliarden Franken. Neben Interessenvertretung betreibt Swico das nationale Rücknahmesystem «Swico Recycling» für Elektronik-Altgeräte.

Für unsere Branche ist ein modernisierter Datenschutz zentral, der Innovation nicht übermässig einschränkt, administrativ tragbar ist und angemessen im Rahmen der internationalen Entwicklungen ausfällt. Die vorliegende Verordnungslösung weist jedoch mehrfache Unstimmigkeiten auf, die es ohne Gefährdung des Zeitplans hinsichtlich der Äquivalenzanerkennung durch die Europäische Union zu bereinigen gilt. Insbesondere ist auf einen Swiss Finish zu verzichten und der Wille des Gesetzgebers zu respektieren.

1. Grundsätzliche Bemerkungen

Das neue Datenschutzgesetz (revDSG) war Gegenstand langer parlamentarischer Diskussionen, an denen unterschiedliche Lager beteiligt waren. Die Wirtschaft hat sich stets für eine administrativ tragbare, gegenüber der EU angemessene Lösung ohne Swiss Finish eingesetzt. Das Ergebnis der Beratungen war eine Kompromisslösung. Der vorliegende Entwurf trägt diesem Kompromiss ungenügend Rechnung. An einzelnen Stellen sind sogar Bestimmungen eingeflossen, welche im Verlauf des Gesetzgebungsprozesses zum revDSG bewusst gestrichen wurden und entsprechend nicht Teil des Schlussabstimmungstextes sind.

Die Bereinigung des vorliegenden E-VDSG sollte so erfolgen, dass der Zeitplan hinsichtlich des Äquivalenzbeschlusses der EU gegenüber der Schweiz nicht gefährdet wird, denn unsere Mitglieder sind in einem besonderen Masse auf einen barrierefreien Datenaustausch mit der EU angewiesen

Unseres Erachtens ist der E-VDSG mit Mängeln durchzogen, welche unter folgenden Oberbegriffen zusammengefasst werden können (detaillierte Erklärungen hierzu sind jeweils unter den Kommentaren zu den einzelnen Bestimmungen angebracht):

- **Swiss Finish muss auch in der VDSG beseitigt werden**: Schweizer Besonderheiten, welche über die europäische Regulierung hinausgehen, schaffen für die Schweizer ICT-Branche sowie für die Gesamtwirtschaft erheblichen administrativen Mehraufwand ohne effektiven Nutzen für Konsumentinnen und Konsumenten. Entsprechend wurde in der Diskussion zum Gesetzgebungsprozess zum revDSG darauf geachtet, derartige Regelungen weitgehend zu vermeide bzw. zu beseitigen. Dies muss auch für die VDSG gelten. Es ist nicht ersichtlich, auf welcher Grundlage der E-VDSG zahlreiche Swiss Finish enthält.
- **Verordnungsbestimmungen ohne hinreichende gesetzliche Grundlage im revDSG:** Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist darauf beschränkt, die Bestimmungen des betreffenden Bundesgesetzes durch Detail-vorschriften näher auszuführen, um zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt hingegen eine entsprechende Delegationsnorm im Gesetz voraus. Vorliegend enthält der E-VDSG viele Bestimmungen, die im Gesetz hätten geregelt werden müssen und nicht auf dem Verordnungswege eingeführt werden können.

- **Politischer Prozess zum revDSG wurde nicht respektiert:** Der E-VDSG versucht Bestimmungen einzuführen, auf die im langwierigen politischen Prozess im Sinne einer Kompromisslösung verzichtet wurde. Zudem enthält er statt notwendiger Klarstellungen praxisfremde Regelungen oder führt parallele Verzeichnispflichten und sonstigen neuen Administrativaufwand ein – ohne erkenntlichen Nutzen. Leider trägt auch der erläuternde Bericht hier nicht zur Klärung bei.

2. Detaillierte Streichungs- und Anpassungsvorschläge

- Art. 2 Schutzziele (Datensicherheit): *Anpassen*.

Mit diesem Artikel wird die bereits bekannte Liste von Schutzzielen erweitert in Bezug auf die Massnahmen zur Gewährleistung der Datensicherheit. Die Liste fällt zu absolut aus: Mit der gewählten Formulierung wird der Eindruck erweckt, dass es sich um absolut zu erreichende Anforderungen handelt. Zu treffen sind angemessene Massnahmen; eine vollständige Sicherheit ist nicht erforderlich. Entsprechend ist der Wortlaut zu ändern und «erreichen» mit «anstreben» zu ersetzen.

Zudem enthält die Bestimmung zu detaillierte Formulierungen. Im Kern muss es im hier zu regelnden Bereich der Datensicherheit um die klassischen Schutzziele Integrität, Verfügbarkeit und Belastbarkeit gehen. Eine generelle Dokumentationspflicht wurde vom Gesetzgeber verworfen. Die Reduktion von lit. a bis lit. k auf die genannten Begriffe stimmt zudem mit Art. 32 DSGVO überein. Andernfalls liegt ein Swiss Finish vor.

- Art. 3 Abs. 1 bis 4 E-VDSG Protokollierung (Datensicherheit): *Streichen*.

Ergibt eine Datenschutz-Folgenabschätzung (DSFA) ein «hohes Risiko», so wird für die Datenbearbeitung mit dieser Norm ein Audit-Trail vorgesehen (Protokollieren von Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten). Die Audit-Trails sind gemäss Verordnungstext für zwei Jahre aufzubewahren (in vom operativen System getrennten Systemen) und die Protokolle dürfen nur für Datenschutzzwecke aufbewahrt werden.

Wir beantragen, diese Norm ersatzlos zu streichen, da sie mit einem massiven Datenbearbeitungsaufwand und schwieriger technischer Umsetzbarkeit einhergeht. Beispielsweise ist nicht klar, wie die Protokollierung des Elements «Lesen» in der Praxis erfolgen soll.

Die Pflicht zur Protokollierung nach Abs. 1 stammt aus der geltenden VDSG und sollte die Nachvollziehbarkeit einer Datenbearbeitung sicherstellen, wenn der Datenschutz nicht eingehalten werden konnte. Diese Ausgangslage gibt es bei der DSFA nicht: Dort muss bei einer Bearbeitung mit hohem Risiko der EDÖB konsultiert werden. Die Protokollierung entfällt dabei, da der Datenschutz in diesem Fall eingehalten wurde. Die Regelung stellt einen Swiss Finish dar und es fehlt die gesetzliche Grundlage dazu. Unklar und offen lässt der neue Verordnungstext, ob die Verletzung der Protokollierungspflicht gegebenenfalls auch eine strafbare Verletzung der Datensicherheit darstellen kann.

Sollte dennoch an dieser Bestimmung festgehalten werden, so müsste auf alle Fälle die Frist für die Pflicht zur Vorhaltung von Sicherheits-Logs auf einem Jahr belassen und nicht neu auf zwei Jahre ausgeweitet werden (Art. 3 Abs. 4 E-VDSG). Eine zweijährige Frist geht über die anerkannte Security Praxis hinaus (z.B. internationale Standards wie NIST 800-92), in der 12 Monate Standard sind für die Vorhaltung von Sicherheitsprotokollen aus Systemen, aus denen ein «hohes Risiko» für die Bearbeitung der personenbezogenen Daten hervorgeht. Durch eine zweijährige Frist würden die Kosten des oben genannten massiven Datenbearbeitungs-volumens unverhältnismässig verdoppelt. Es ist zu betonen, dass Protokollierungen insbesondere zur raschen Aufdeckung von Sicherheitsverletzungen dienen und nur in Zusammenhang mit einem Intrusion Detection and Prevention System (IDPS) Sinn machen, was zwar in den TOMs unter Art. 2 E-VDSG angesprochen wird, jedoch nicht in den Kontext der Protokollierung gesetzt wird.

- Art. 4 Abs. 1 bis 3 E-VDSG Bearbeitungsreglement von privaten Personen (Daten-sicherheit): *Streichen*.

Diese Bestimmung sieht die Pflicht zur Führung eines Bearbeitungsreglements vor, wenn besonders schützenswerte Personendaten umfangreich bearbeitet werden oder bei einem Profiling mit hohem Risiko. Für dieses Bearbeitungsreglement werden Mindestangaben vorgesehen (z.B. Angaben zu den Massnahmen, die zur Datenminimierung getroffen wurden).

Wir beantragen diesen Artikel zur Streichung, da er einen unnötigen administrativen Mehraufwand in Form eines separaten Zusatzdokuments fordert, das der Verantwortliche unterhalten muss. Die Norm verwischt die Grenzen zwischen etablierten Instrumenten wie DSFA, Bearbeitungsverzeichnis, Datenschutztraining und internen Richtlinien und ist unnötig. Diese haben sich in der Praxis als effektive Mittel bewährt. Die Bestimmung schafft insbesondere eine unnötige Doppelspurigkeit zum Verzeichnis der Bearbeitungstätigkeiten nach Art. 12 revDSG. Im erläuternden Bericht ist nicht ersichtlich, worin der Mehrwert des neuen Bearbeitungsreglements gesehen wird. Auf eine Bestimmung dieser Art wurde zudem im Laufe des Vernehmlassungsprozesses bewusst verzichtet, was zu respektieren ist. Auch hier ist eine fehlende Rechtsgrundlage im revDSG festzustellen: Art. 8 revDSG regelt nur die Datensicherheit i.e.S. und nicht die Einhaltung der Bearbeitungsgrundsätze, worauf Art. 4 E-VDSG abzielt. Bereits für die Vorgängernorm in der aktuellen VDSG fehlte eine gesetzliche Grundlage, weshalb sie toter Buchstabe blieb. Zudem handelt es sich beim Inhalt dieser Bestimmung erneut um einen Swiss Finish.

Sollte an der Bestimmung dennoch festgehalten werden, so ist es zentral, den Anwendungsbereich auf den Verantwortlichen einzuschränken und nicht auch auf den Auftragsbearbeiter auszuweiten (Abs. 1). Dies ist auch unter bisherigem Recht der Fall («Inhaber der Datensammlung» gem. Art. 11 VDSG) und notwendig, um die Grenzen der Rechenschaft zwischen dem Verantwortlichen und dem Auftragsbearbeiter nicht zu verwässern.

- Art. 5 Abs. 1 bis 3 E-VDSG: Bearbeitungsreglement von Bundesorganen: *Streichen.*

Art. 5 E-VDSG hält fest, dass Bundesorgane und deren Auftragsbearbeiter in den Fällen von Abs. 1 lit. a bis f für sämtliche automatisierten Datenbearbeitungen ein Bearbeitungsreglement erstellen müssen. Für das Bearbeitungsreglement werden dieselben Mindestangaben wie bei den Privaten vorgesehen.

Wir beantragen die Streichung des Artikels aus den gleichen Gründen, die bereits bei Art. 4 E-VDSG für Private aufgeführt wurden: Der Anwendungsbereich würde für Bundesorgane praktisch für jede automatisierte Bearbeitung gelten. Zu einem Zusatznutzen führt die Bestimmung auch bei Bundesorganen nicht, da die bereits etablierten Dokumentationspflichten wie die DSFA oder Bearbeitungsverzeichnisse auch für Bundesorgane gelten. Analog den Ausführungen zu Art. 4 E-VDSG fehlt es auch dieser Bestimmung an der gesetzlichen Grundlage.

- Art. 6 E-VDSG Modalitäten der Bearbeitung durch den Auftragsbearbeiter. *Streichen Abs. 1 und 2, Klarstellen Abs. 3.*

Art. 6 Abs. 1 E-VDSG hält fest, dass der Verantwortliche, welcher die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, für den Datenschutz verantwortlich bleibt. Dabei muss er sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.

Für den Verantwortlichen ist es in der Praxis nicht möglich, das Kriterium der «Sicherstellung» betreffend die vertrags- und gesetzesgemässe Bearbeitung zu erfüllen. Er kann höchstens dazu «Sorge tragen». Diese Unterscheidung ist wesentlich, da der Verantwortliche datenschutzrechtlich haftbar bleibt, zivilrechtlich jedoch nur bei Verschulden (Art. 41 ff. OR) und nicht etwa kausal. Die vorliegende Einrichtung einer Kausalhaftung ist nicht nötig, da die allgemeinen Haftungsregeln nach OR greifen. Auch hier fehlt unseres Erachtens eine Rechtsgrundlage im revDSG und wir sehen hier erneut einen Swiss Finish.

Art. 6 Abs. 2 E-VDSG hält weiter fest, dass – im Falle des Nichtunterliegens des Auftragsdatenbearbeiters unter das DSG – der Verantwortliche sich bei einem Auslandtransfer vergewissern muss, dass andere gesetzliche Datenschutzbestimmungen mit demselben Niveau greifen oder dieses vertraglich sicherstellen. Wir beantragen auch diesen Absatz zur Streichung, da keine Notwendigkeit besteht: Auslandtransfers sind abschliessend in Abschnitt 3 revDSG geregelt. Zudem regelt Abs. 2 den Gegenstand des Auslandtransfers nur ungenügend bzw. nicht abschliessend.

Art. 6 Abs. 3 E-VDSG hält schliesslich für Bundesorgane fest, dass der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen darf, wenn das Bundesorgan als Verantwortlicher dies schriftlich genehmigt hat. Diesbezüglich ist explizit klarzustellen, dass eine Genehmigung auch in elektronischer Textform genügt und sie in allgemeiner Form erfolgen kann (analog der DSGVO). Die Ausführungen in der Botschaft zu Art. 6 Abs. 3 E-VDSG lassen dies klar zu. Dienste von Standard-Online-Providern, welche durch Bundesorgane bezogen werden, sehen ausschliesslich diese Methode vor.

- Art 7 E-VDSG Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans: *Streichen oder anpassen.*

Nach Art. 7 E-VDSG müssten Datenschutzberaterinnen oder -Berater von Bundesorganen den EDÖB umgehend informieren über den Abschluss von Auftragsdatenbearbeitung, die Genehmigung der Übertragung von Datenbearbeitungen an Dritte oder über allgemeine Probleme bei der Einhaltung von Datenschutzvorschriften. Mit Art. 29 E-VDSG besteht bereits eine Informationspflicht, welche allgemeiner formuliert ist und auch die Auftragsbearbeitungen umfasst, sofern diese relevant sind. Welche «Probleme» zu melden sind, ist zudem unklar. Deshalb beantragen wir die Streichung oder eventualiter die entsprechende Anpassung der Bestimmung.

- Art. 8 E-VDSG Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs (Bekanntgabe von Personendaten ins Ausland): *Anpassen*.

Der Bundesrat legt nach Art. 16 Abs. 1 revDSG fest, welche Staaten oder internationalen Organisationen einen angemessenen Datenschutz gewährleisten. Die vorliegende Bestimmung kann jedoch in einer Art missverstanden werden, dass die verantwortliche Stelle und nicht der Bundesrat die Angemessenheit des Datenschutzes im Empfängerstaat feststellen muss. In Art. 8 E-VDSG ist deshalb klar zum Ausdruck zu bringen, dass sich diese Bestimmung ausschliesslich an den Bundesrat richtet.

- Art. 9 E-VDSG Datenschutzklauseln und spezifische Garantien (Bekanntgabe von Personendaten ins Ausland): *Streichen Abs. 1 und Abs. 2.*

Diese Bestimmung legt inhaltliche Vorgaben für Datenschutzklauseln zum Schutz von Personendaten in unsicheren Drittländern fest (z.B. Einhaltung der Bearbeitungsgrundsätze, Namen der Empfängerstaaten, Anforderungen an die Aufbewahrung und Löschung von Daten).

Der Anwendungsbereich dieser Bestimmung bezieht sich auf die Standardvertragsklauseln der EU-Kommission (SCC), welche in der Praxis überwiegend verwendet werden. Abs. 1 sollte entsprechend keine Vorgaben machen, die mit den SCC nicht konform sind. Die DSGVO leistet einen angemessenen Schutz. Dieser ist für Datenbekanntgaben durch Schweizer Verantwortliche ebenso gut. Deshalb ist der Abs. 1 unseres Erachtens überflüssig.

Abs. 2 sieht die Pflicht des Verantwortlichen vor, sicherzustellen, dass der Empfänger im Ausland diese Datenschutzklauseln auch einhält. Diese Bestimmung ist ersatzlos zu streichen: Abs. 2 ist zu unbestimmt, da nicht hervorgeht, was diese Massnahmen sein könnten. Neben der unrealistischen Regelungsabsicht fehlt es an einer gesetzlichen Grundlage, und auch die DSGVO kennt keine solche Regelung.

- Art. 10 Abs. 1 E-VDSG Standardschutzklauseln (Bekanntgabe von Personendaten ins Ausland): *Streichen.*

Abs. 1 dieser Bestimmung (der Exporteur trifft angemessene Massahmen, um sicherzustellen, dass der Importeur die Klauseln beachtet) ist durch die neuen SCC eigentlich überflüssig geworden. Sie ist zudem zu unbestimmt und es ist nicht klar, was diese Massnahmen sein könnten. Der Exporteur kann in der Praxis nicht sicherstellen, dass der Empfänger die Klauseln beachtet. Er kann es nur verlangen und im Rahmen der neuen SCC (Klausel 14) prüfen, ob lokales Recht der Einhaltung entgegensteht. Dieser Verordnungsbestimmung fehlt es zudem ebenso an der gesetzlichen Grundlage.

- Überschrift «2. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters»: *Kürzen.*

Den Auftragsbearbeiter treffen keine gesetzlichen Informationspflichten, weshalb dieser aus der genannten Überschrift zu streichen ist.

- Art. 13 E-VDSG Modalitäten der Informationspflichten (Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters): *Streichen des Auftragsdatenbearbeiters in Abs. 1 und Streichen von Abs. 2.*

Diese Bestimmung hält in Abs. 1 eine Informationspflicht für den Auftragsdatenbearbeiter fest. Dieser ist jedoch nicht Gesetzesadressat, es treffen ihn keine gesetzlichen Informationspflichten und er kann nicht auf dem Verordnungsweg in Pflicht genommen werden. Eine Informationspflicht des Auftragsdatenbearbeiters würde seiner Weisungsbindung widersprechen. Art. 19 revDSG geht klar von der Alleintragung des Verantwortlichen aus, insofern hier die Grenzen zum Auftragsdatenbearbeiter verwischt werden. Vielmehr steht der Verantwortliche in der Pflicht, durch Auswahl und Instruktion des Auftragsbearbeiters für eine entsprechende Erfüllung von Art. 19 revDSG zu sorgen. Abs. 1 äussert sich weiter zur Ausgestaltung der Informationspflicht. Leider wird im erläuternden Bericht nicht klargestellt, dass eine Datenschutzerklärung auf der Website in der Regel genügt – im Gegenteil. Auch enthält der erläuternde Bericht praxisfremde Empfehlungen (z.B. eine Empfehlung, am Telefon den Link zur Datenschutzerklärung zu nennen). Abs. 1 in Kombination mit den Erläuterungen ist gesamthaft unpräzise, führt zu Rechtsunsicherheit und es fehlt an einer Auseinandersetzung mit den wesentlichen Fragen in diesem Bereich.

Die Bestimmung in Abs. 2 ist ersatzlos zu streichen: Der EDÖB hat keine gesetzliche Regelungskompetenz bei der Ausgestaltung von Piktogrammen. Die Entwicklung von Piktogrammen ist Sache der Verantwortlichen. Die vorgeschlagenen Vorgaben würden die Einführung der aus Datenschutzsicht grundsätzlich vorteilhaften Piktogramme unnötig erschweren oder gar verhindern. Die «Maschinenlesbarkeit» ist ein irritierendes Kriterium, für das es keinen Standard gibt. Gesamthaft fehlt es der Norm an der gesetzlichen Grundlage, und es ist offengelassen, ob eine Strafbarkeit möglich ist.

- Art. 14 E-VDSG Informationspflicht der Bundesorgane bei der systematischen Beschaffung von Personendaten (Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters): *Präzisierung.*

Die Bestimmung sieht vor, dass das verantwortliche Bundesorgan bei der systematischen Beschaffung von Personendaten die betroffene Person auf die Freiwilligkeit der Auskunftserteilung hinweist, falls diese zur Auskunft nicht verpflichtet ist. Diese Bestimmung ist praxisfremd, da die Freiwilligkeit häufig aus den Umständen hervorgeht. Entsprechend ist der Wortlaut zu ergänzen mit « (...) soweit dies nicht aus den Umständen ersichtlich ist».

- Art. 15 E-VDSG Information bei der Bekanntgabe von Personendaten (Pflichten des Verantwortlichen): *Streichen.*

Bei der Bekanntgabe von Personendaten muss der Empfänger gemäss dieser Bestimmung über Aktualität, Zuverlässigkeit und Vollständigkeit der bekanntgegebenen Daten informiert werden. Der Einbezug des Auftragsarbeiters ist wiederum nicht vom revDSG abgedeckt (fehlende gesetzliche Grundlage) und die Bestimmung ist nicht praktikabel. Letztlich ist es Sache des Verantwortlichen, die Einhaltung der Datenschutzgrundsätze sicherzustellen. Dieser kann eine Angabe der Aktualität und dergleichen von Personendaten verlangen, aber nicht in allen Fällen. Eine harte Pflicht zu einer solchen Information kann in der Praxis nicht umgesetzt werden. Zudem wäre auch das wieder ein Swiss Finish.

- Art. 16 E-VDSG Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten (Pflichten des Verantwortlichen): *Streichen oder eventualiter Begrenzung der Mitteilungspflicht auf weitergegebene Daten.*

Gemäss dieser Bestimmung informiert der Verantwortliche den Empfänger von bekanntgegebenen Personendaten unverzüglich über Berichtigung, Löschung, Vernichtung sowie Einschränkung der Bearbeitung von Personendaten. Diese Bestimmung ist ersatzlos zu streichen, da sie im Entwurf zum revDSG zwar vorgesehen, aber durch das Parlament gestrichen wurde. Eine Wiedereinführung auf dem Verordnungstext würde den Willen des Gesetzgebers missachten. Die Bestimmung scheint sich betreffend die Einschränkung der Bearbeitung an Art. 18 der DSGVO anzulehnen, obwohl das revDSG dieses Betroffenenrecht nicht kennt und keine gesetzliche Grundlage dafür anbietet. Die entsprechenden Pflichten werden bereits durch die Bearbeitungsgrundsätze vorgegeben und (via Vertragsvorgaben) an die Empfänger weitergegeben. Bei den heutigen systembedingten Bearbeitungen werden korrigierte/ gelöschte Daten für die Empfänger regelmässig systembedingt aktualisiert, damit die richtigen Daten bearbeitet werden können.

Wird die Bestimmung überarbeitet und beibehalten, so muss die Mitteilungspflicht zwingend auf weitergegebene Daten begrenzt werden. Bei allen anderen Daten erscheint dies nicht sachgerecht, weshalb Art. 16 E-VDSG entsprechend präzisiert werden müsste.

- Art. 19 E-VDSG Meldung der Verletzungen der Datensicherheit (Pflichten des Verantwortlichen): *Streichen Abs. 5.*

Abs. 5 dieser Bestimmung hält Dokumentationspflichten für den Verantwortlichem im Falle einer Verletzung der Datensicherheit fest und macht Vorgaben zur inhaltlichen Ausgestaltung. Leider geht weder aus dem Normtext noch aus den Erläuterungen hervor, wozu diese dient. Aus der Gesetzessystematik ergibt sich grundsätzlich, dass nur Verletzungen zu dokumentieren sind, welche eine Meldepflicht gegenüber dem EDÖB begründen, nicht Verletzungen unterhalb der Meldeschwelle. Abs. 5 hält zudem fest, dass «alle mit den Vorfällen zusammenhängenden Tatsachen» gemeldet werden müssen. Dies ist in der Praxis nicht möglich: Die Dokumentationspflicht kann nur bekannte Fälle abdecken; der Verantwortliche ist nicht gehalten, weitere Nachforschungen anzustellen.

Zudem ist die dreijährige Frist zwecks Dokumentierung unverhältnismässig lange gewählt: Die Frist ist auf ein Jahr zu begrenzen, sollte Abs. 5 nicht gestrichen werden. Der Absatz entbehrt zudem einer gesetzlichen Grundlage im revDSG und ist lediglich aus der DSGVO bekannt.

- Art. 20 E-VDSG Modalitäten (Auskunftsrecht der betroffenen Person): *Anpassen Abs. 1, 3 und 5.*

Abs. 1 hält fest, dass das Auskunftsbegehren schriftlich zu stellen sei und dass, «wenn alle einverstanden sind», das Begehren auch mündlich gestellt werden kann. Diese Regelung ist in der Praxis wenig hilfreich: Ein Auskunftsbegehren kann immer mündlich gestellt werden, nur muss der Verantwortliche bei mündlichen Begehren nicht reagieren. Wenn schon, dann müsste der Wortlaut gemäss unseren Mitgliedern explizit dahingehend ergänzt werden, dass ein Begehren nicht nur schriftlich, sondern auch elektronisch gestellt werden kann. Dies ist zwar bereits in den Erläuterungen zur Verordnung festgehalten, sollte aber aufgrund des hohen Stellenwerts auch im Wortlaut des Artikels selbst klargestellt werden.

Nach Abs. 3 muss die Auskunft für die betroffene Person verständlich sein: Es handelt sich hierbei um einen Swiss Finish und es ist nicht klar, wann eine Auskunft «verständlich» ist. Es stellt sich beispielsweise die Frage, was dem Teilnehmer einer medizinischen Studie erklärt werden muss, der alle von ihm erhobenen Daten anfragt. Ob eine Auskunft verständlich ist, liegt in erster Linie am Empfängerhorizont und es wäre unzumutbar, dass auf besondere Schwächen des konkreten Auskunftsstellers eingegangen werden muss. Massgeblich wäre der Durchschnitts-Betroffene.

Gemäss Abs. 5 hat der Verantwortliche die Dokumentation über die Gründe für eine Verweigerung, einen Aufschub oder eine Einschränkung des Auskunftsrechts mindestens für drei Jahre aufzubewahren. Auch diese Dokumentationsfrist ist unverhältnismässig lange gewählt und ist auf ein Jahr zu begrenzen.

- Art. 21 E-VDSG Zuständigkeit (Auskunftsrecht der betroffenen Person): *Anpassen Abs. 2.*

Diese Norm regelt in Abs. 1 die Zuständigkeit für die Gewährung des Auskunftsrechts bei mehreren Verantwortlichen. Abs. 2 bezieht sich auf Daten, die von einem Auftragsdatenbearbeiter bearbeitet werden: Der Verantwortliche hat ihm das Auskunftsbegehren weiterzuleiten, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen. Besser wäre es unserer Ansicht nach, den Auftragsdatenbearbeiter zu verpflichten, den Verantwortlichen dabei zu unterstützen, die Auskunft zu erteilen. Diese Lösung ist in der Praxis entsprechend vertraglich geregelt. Auftragsbearbeiter sind in der Regel nicht darauf eingerichtet, Auskunft zu erteilen, weil sie keine gesetzliche Pflicht trifft. Der vorliegende Verweis auf den Auftragsbearbeiter kann in der Praxis deshalb Probleme schaffen. Zudem kann ein Verantwortlicher es sich aus Compliance-Gründen nicht leisten, die Auskunft einfach weiterzuleiten statt die notwendigen, internen Prozesse aufzubauen. Leidtragend wären die betroffenen Personen. Die Verpflichtung zur Auskunftserteilung muss klar zugewiesen werden. Der Wortlaut von Abs. 2 ist entsprechend anzupassen.

- Art. 23 E-VDSG Ausnahmen von der Kostenlosigkeit (Auskunftsrecht der betroffenen Person: *Anpassen Abs. 1 i.V.m. Abs. 2.*

Abs. 1 legt eine angemessene Beteiligung an den Kosten fest, wenn die Auskunftserteilung mit unverhältnismässigem Aufwand verbunden ist. Abs. 2 legt die Obergrenze der Beteiligung für die gesuchstellende Person auf CHF 300.- fest. Besonders für kleinere Firmen wäre eine Erhöhung der Obergrenze relevant, da grössere Firmen in der Regel über etablierte Prozesse zwecks Auskunftserteilung ohne erheblichen Mehraufwand verfügen. Zudem fehlt in Abs. 1 die Klarstellung und Ergänzung, dass auch querulatorische Auskunftsbegehren unter die Bestimmung fallen.

- Art. 25 E-VDSG Datenschutzberaterin oder Datenschutzberater: *Klarstellen.*

Die Norm äussert sich zu den Kompetenzen eines privaten Datenschutzberaters und hält fest, welche Ressourcen und Befugnisse der Verantwortliche der privaten Datenschutzberaterin zur Verfügung stellen muss. Leider fehlt die Abstimmung zwischen Gesetz und Verordnung. Das Pflichtenheft wurde nicht aus dem revDSG übernommen, sondern aus der bisherigen Verordnung. Im revDSG werden bereits Schulung, Beratung und Mitwirkung an der Compliance genannt, womit fraglich ist, ob es die entsprechende Regelung in der VDSG überhaupt braucht. Zudem fällt auf, dass die Aufgaben als persönliche gesetzliche Pflicht der privaten Datenschutzberaterin aufgeführt werden, was haftungsrechtliche Fragen ohne entsprechende Klärung nach sich zieht. In den genannten Punkten ist eine Klarstellung bzw. Überarbeitung notwendig.

- Art. 26 E-VDSG Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten: *Klarstellen.*

Gemäss dieser Bestimmung kann der Bundesrat bei Unternehmen mit weniger als 250 Mitarbeiterinnen und Mitarbeitern Ausnahmen von der Inventarpflicht vorsehen, sofern nicht «umfangreich besonders schützenswerte Personendaten bearbeitet werden» und nicht ein «Profilig mit hohem Risiko» durchgeführt wird. Es ist im Umkehrschluss nicht klar, ob nun nur diese beiden Fälle ein hohes Risiko mit sich bringen. Zudem ist klarzustellen, ob dies auch der Massstab ist, wann eine Datenschutz-Folgenabschätzung durchzuführen ist. Unklar ist auch, ob bei Nichterfüllen einer der genannten Ausnahmen ein Inventar für sämtliche Aktivitäten zu erstellen ist.

- Art. 32 Abs. 1 E-VDSG Meldung an den EDÖB (Projekte von Bundesorganen zur automatisierten Bearbeitung): *Streichen*

Die Bestimmung sieht vor, dass Bundesorgane geplante automatisierte Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung dem EDÖB melden müssen. Dies führt zu einem erheblichen Mehraufwand für die Dokumentation, insbesondere da jede automatisierte Bearbeitung und nicht nur solche mit einem (potenziellen) hohen Risiko gemeldet werden müssen. Weiter sind im vorgesehenen Meldezeitpunkt die verlangten Angaben in aller Regel noch nicht genügend detailliert vorhanden. Nicht zuletzt fehlt der Bestimmung auch die gesetzliche Grundlage im revDSG. Wir beantragen diese Norm zur ersatzlosen Streichung.

- 7. Kapitel Schlussbestimmungen: *Anpassen*

Das Regime der Übergangsbestimmungen auf Stufe revDSG fällt lückenhaft aus, weshalb eine Anpassung auf Verordnungsstufe zu erfolgen hat. Für sämtliche neuen Pflichten, welche erheblichen Aufwand generieren, müssen angemessene Übergangsfristen bestehen. Der etablierte Erfahrungswert für einen angemessenen Zeitraum liegt bei zwei Jahren (analog DSGVO). Im revDSG liegt der Fokus jedoch nicht, wie in der DSGVO, auf Übergangsfristen für das Gesamtpaket, sondern auf einzelnen Regeln und Pflichten.

Im revDSG bestehen einige neue Pflichten, für die keine Übergangsfrist festgelegt wurde: Art. 8 revDSG (Pflicht, eine angemessene Datensicherheit zu gewährleisten), Art. 12 revDSG (Pflicht zur Erstellung eines Datenbearbeitungs-Verzeichnisses) und Art. 24 i.V.m. Art. 19 revDSG (Meldepflicht bei Verletzung der Datensicherheit). Für diese drei Pflichten wäre, unter Berücksichtigung des Erhalts der Äquivalenzanerkennung, eine Übergangsfrist bis mindestens anfangs 2023 notwendig. Die Anpassung in der Verordnung könnte mittels eines neuen, spezifischen Artikels bei den Schlussbestimmungen oder mittels einer Verschiebung des Inkrafttretens des Gesamtpakets (revDSG und E-VDSG) auf anfangs 2023 erreicht werden.

Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Andreas Knöpfli
Präsident

Ivette Djonova
Head Legal & Public Affairs

swimag GmbH
Mattenstrasse 14
CH-5436 Würenlos

Einschreiben
Bundesamt für Justiz
Bundesrain 20
CH-3003 Bern

Vorab per Mail: jonas.amstutz@bj.admin.ch, info@bj.admin.ch

Vernehmlassung bzw. Stellungnahme zum:

- **Entwurf zur Verordnung zum Bundesgesetz über den Datenschutz;**
- **bzw. E-VDSG.**

Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Gestützt auf das Vernehmlassungsgesetz (VlG) und die Vernehmlassungsverordnung (VlV) wie auch unseren gesammelten Praxiserfahrungen gerade im Zusammenhang mit dem Datenschutz ersuchen wir Sie im Rahmen des vorbezeichneten Vernehmlassungsverfahrens bzw. -prozesses als Zugehörige der interessierten Kreise höflich um Kenntnisnahme und geneigte Berücksichtigung der folgenden Ausführungen, wobei die jeweiligen *rechtlichen Bestimmungen kursiv und darin weiter angebrachte Änderungswünsche* ***fett*** *oder* ~~*durchgestrichen*~~ sowie nachfolgend zugehörige Kommentare "normal", also ohne Schriftauszeichnung, erscheinen.

Art. 1 Abs. 1 lit. c

der Stand der ***Wissenschaft und*** *Technik;*

Die Präsenz des Standes der Wissenschaft stellt gegenüber der Technik in nahezu jedem erdenklichen Fall ein anzustrebendes deutlich höheres Mass an Sicherheit dar und bereitet aufgrund der quasi überall uneingeschränkten Verfügbarkeit keine zusätzlichen Hemmnisse. Im Übrigen gehört der Stand der Wissenschaft im Qualitätswesen und der Produkthaftung seit mehreren Jahrzehnten zum allseits bewährten und geschätzten Standard. Warum sollte er dann bei solch einem wichtigen Thema wie dem Datenschutz fehlen?

Art. 1 Abs. 1 lit. d

~~*Implementierungskosten.*~~

der jeweils zur Implementierung wie Installation mindestens vorzusehenden Mittel, Aufwände und Kosten.

***Art. 2** Schutzziele*

~~*Soweit angemessen,*~~

*Die Massnahmen zur Gewährleistung der Datensicherheit müssen **mindestens** folgende Schutzziele erreichen:*

Art. 2 lit. a

*Zugriffskontrolle: Der Zugriff **der jeweils auf ein Minimum zu reduzierenden** berechtigten Personen ist auf **das Notwendigste** ~~die~~**der**jenigen Personendaten beschränkt, die sie **unbedingt und zwingend** zur Erfüllung ihrer Aufgabe benötigen.*

In der Vergangenheit gab es immer wieder Fälle, wo ohne erkennbaren Grund einfach die Zahl der berechtigten Personen in nicht nachvollziehbarer Art und Weise Erhöhung fand und diese zudem damit Operationen vornahmen, was nicht in den Erfüllungsbereich ihrer Aufgaben gehörte. Um derartigen Missbrauch gleich von vornherein zu begegnen, bietet sich u.a. die zuvor vorgeschlagene strengere Formulierung von Art. 2 Abs. lit. a an.

Art. 2 lit. b

*Zugangskontrolle: Der Zugang zu **physischen wie virtuellen** Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen **gleich von vornherein und von allem Anfang an** verwehrt.*

Art. 2 lit. c

*Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben, **Beschreiben, Zerstören** oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht.*

Art. 2 lit. g

*Eingabekontrolle: In automatisierten Systemen ~~kann~~ **lässt sich jederzeit überprüfen** ~~überprüft werden~~, welche Personendaten zu welcher Zeit und **zu welchem Zweck bzw. aufgrund welcher gesetzlichen Grundlage** von welcher Person eingegeben oder verändert wurden.*

Art. 2 lit. h

Bekanntgabekontrolle: Es ***lässt sich jederzeit überprüfen*** ~~*kann überprüft werden*~~*, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden.*

Art. 2 lit. i

Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen ~~*kann*~~ ***lässt sich*** *bei einem physischen,* ~~*und*~~ *technischen* ***oder sonstigen datengefährdenden*** *Zwischenfall* ***bzw. Angriff unverzüglich ohne jegliche Beeinträchtigung vollumfänglich wiederherstellen.*** ~~*wiederhergestellt werden.*~~

Art. 2 lit. k

Erkennung: Verletzungen der Datensicherheit ***müssen sich unverzüglich erkennen*** ~~*können rasch erkannt*~~ *und Massnahmen zur* ~~*Minderung oder*~~ ***erfolgreichen wie vollständigen*** *Beseitigung der Folgen* ***unmittelbar einleiten lassen***. ~~*eingeleitet werden.*~~

Art. 3 Abs. 1 *Protokollierung*

Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein ~~*hohes*~~ *Risiko für* ***Persönlichkeits- oder Grundrechtsverletzungen*** ~~*die Persönlichkeit oder die Grundrechte*~~ *der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten* ***sowie die jeweilige Zweckbindung bzw. den genauen Bearbeitungsgrund.***

Art. 3 Abs. 2

Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten ***sowie die jeweilige Zweckbindung bzw. den genauen Bearbeitungsgrund.***

Art. 3 Abs. 3

Die Protokollierung gibt Aufschluss über die Art, ***Zweck, Grund und rechtliche Legitimation bzw. Verhältnismässigkeit*** *des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.*

Art. 3 Abs. 4

*Die Protokolle sind während **fünf** Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, **als zweifache Kopie an zwei unabhängig voneinander gesondert gesicherten Orten** aufzubewahren. Sie sind ausschliesslich **auf begründeten Antrag den von der Datenbearbeitung betroffenen Person oder Personen und** den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.*

In Anbetracht der geltenden Verjährungsfrist von 5 Jahren für eine Vielzahl von Forderungen erscheint auch hier eine mindestens fünfjährige Aufbewahrungsfrist mehr als gerechtfertigt.

Art. 4 Abs. 1 lit. a

~~umfangreich~~ besonders schützenswerte Personendaten bearbeiten; oder

Gerade bei geringfügiger und vereinzelter Bearbeitung besonders schützenswerter Personendaten braucht es für dieses Thema eine hinreichende Sensibilisierung, was unter anderem durch das dann auch notwendige Erstellen eines entsprechenden Bearbeitungsreglementes Ausdruck findet.

Art. 4 Abs. 1 lit. b

*~~ein~~ Profiling**s** ~~mit hohem Risiko~~ durchführen.*

Art. 4 Abs. 3

*~~?Die private Person?~~ **?Der Verantwortliche und dessen Auftragsbearbeiter?** muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.*

Art. 8 Abs. 1 lit. f

die durch die Bekanntgabe von Personendaten ins Ausland betroffene bzw. damit in Zusammenhang stehende Person oder Personen dürfen keine daraufhin bedingten Benachteiligungen gegenüber einer Nichtbekanntgabe erfahren und im Fall möglicher diesbezüglicher Zweifel gilt es zuvor durch Rechtsvergleiche und Konformitätsprüfungen sicherzustellen, dass im Datenempfängerstaat oder der betreffenden Staatengemeinschaft aufgrund einer vom schweizerischen Recht abweichenden Begriffs- wie Rechtsauffassung, -auslegung, -praxis und -sprechung nicht Gefahr droht, Entscheide zuungunsten der betroffenen Personen und ihrer Rechtsstellung wie -ansprüche nach schweizerischen Massstäben zu riskieren.

Die Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, nutzt wenig ohne die hier unter Art. 8 Abs. lit. f eingefügten Kriterien.

Art. 8 Abs. 1 lit. g

in jedem Fall einer Bekanntgabe von Personendaten ins Ausland braucht es die schriftlich erklärte Zustimmung der betroffenen Person oder Personen.

Art. 8 Abs. 4

~~*Dieser neue Entscheid hat keine Auswirkungen auf bereits erfolgte Datenbekanntgaben.*~~
Diesen neuen Entscheid gilt es auch auf bereits erfolgte Datenbekanntgaben so weit als möglich zu übertragen und vergangene wie Folgeschäden bzw. -verletzungen abzuwenden, auszugleichen oder zu heilen.

Art. 9 Abs. 1 lit. k Ziff. 5

Das Recht auf Nichtzustimmung der Datenbearbeitung.

Art. 12 *Verhaltenskodizes und Zertifizierungen*

Analog zur Frage der im Ausland umzusetzenden Datenschutznormen unter besonderer Berücksichtigung der dort herrschenden Rechtsauslegung wie -praxis (s.a. Bemerkungen zu Art. 8 Abs. 1 lit. f) geht es hier um die Sicherstellung des Datenschutzes u.a. durch Vorweisen einer Zertifizierung der betreffenden ausländischen Organisation. Ob diese Organisation beispielsweise das DSG, die VDSG oder gar die DSGVO der EU erfüllt, erschliesst sich aber keinesfalls aus deren Zertifizierung, selbst nicht nach ISO 27000 ff. Letzteres besagt bestenfalls, dass die Organisation im Ausland die dort geltenden Bestimmungen erfüllt. An die Zertifizierung wie auch Verhaltenskodizes gilt es also besondere Bedingungen unter vollständigem Einbezug der schweizerischen Gesetzgebung bzw. des DSG, der VDSG und der DSGVO zu stellen.

Art. 19 Abs. 1 *Meldung von Verletzungen der Datensicherheit*

Der Verantwortliche meldet dem EDÖB ***und den betroffenen Personen*** *bei einer Verletzung der Datensicherheit:*

Art. 19 Abs. 3

Der Verantwortliche teilt den betroffenen Personen in einfacher und verständlicher Sprache sämtliche Informationen nach Absatz 1 Buchstaben ***a bis g*** ~~*a, e, f und g*~~ *mit.*

Art. 19 Abs. 5 Satz 2

Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens ***fünf*** ~~*drei*~~ *Jahre aufzubewahren.*

In Anbetracht der geltenden Verjährungsfrist von 5 Jahren für eine Vielzahl von Forderungen erscheint auch hier eine mindestens fünfjährige Aufbewahrungsfrist mehr als gerechtfertigt.

Art. 20 Abs. 4 Satz 3

Das persönliche Unterzeichnen des Auskunftsbegehrens durch die betroffene Person mittels qualifiziert zertifizierter elektronischer Signatur gemäss ZertES und OR Art. 14 bzw. Vorweisen der E-ID gilt als hinreichende Identifikation.

Art. 20 Abs. 5 Satz 2

Die Dokumentation ist mindestens ***fünf*** ~~*drei*~~ *Jahre lang aufzubewahren.*

In Anbetracht der geltenden Verjährungsfrist von 5 Jahren für eine Vielzahl von Forderungen erscheint auch hier eine mindestens fünfjährige Aufbewahrungsfrist mehr als gerechtfertigt.

Art. 22 Abs. 3 *Frist*

Durch Zustimmung der betroffenen Person zum elektronischem Austausch bzw. Verkehr und Vorlage des Auskunftsbegehrens unterzeichnet mittels qualifiziert zertifizierter elektronischer Signatur gemäss ZertES und OR Art. 14 bzw. Vorweisen der E-ID einschliesslich Anbringen eines Eilvermerkes verkürzt sich die Auskunftsfrist auf 3 Tage.

In der heutigen Zeit besteht vielfach unmittelbarer Handlungsbedarf bzw. die betroffene Person benötigt häufig die entsprechenden Auskünfte unverzüglich aus Beweissicherungsgründen oder um ihre Ansprüche noch rechtzeitig geltend machen zu können. Unter den aktuell gegebenen technischen Möglichkeiten sollte es bei Zustimmung der betroffenen Person zur elektronischen Übermittlung bzw. Herausgabe kein Problem darstellen, innerhalb von 3 Tagen die nötigen Informationen zur Verfügung zu stellen , also die entsprechenden Auskünfte zu erteilen.

~~***Art. 23*** *Ausnahmen von der Kostenlosigkeit*~~

Den gesamten Art. 23 gilt es unbedingt vollumfänglich zu streichen, da sich quasi jede noch so einfache Auskunftshandlung in Verbindung mit den rechtlich vielfach gebilligten Ausschöpfungsmöglichkeiten des Ermessensspielraumes in der Praxis als unverhältnismässig hoher Datenoffenlegungsaufwand deklarieren lässt und somit gerade gegenüber finanziell nicht gut gestellten betroffenen Personen zum Missbrauch einläd, wie faktische Aktenverweigerung und damit einhergehenden Gehörverletzungen. Auf der anderen Seite die Kostenerhebung mit querulatorischem Verhalten in Verbindung zu bringen oder gar begründen zu dürfen, wie im erläuternden Bericht zum E-VDSG regelrecht herausgefordert, verbietet sich von allem Anfang an, da es an der gesetzlichen Definition des Querulanten fehlt und eine derartige Folge von vornherin in den Bereich der Fehlerhaftigkeit, Missbräuchlichkeit und Diskriminierung von voll geschäfts- und prozessfähigen betroffenen Personen führt.

Art. 24

*Die Artikel ~~20 Absätze 1, 4 und 5~~ **20 bis 22** ~~23~~ sind auf das Recht auf Datenherausgabe und -übertragung sowie deren Einschränkungen sinngemäss anwendbar.*

~~***Art. 26** Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten*~~

Derartige Ausnahmen gilt es von vornherein zu unterbinden, denn nur zu leicht lässt sich mit dieser Ausnahmeregel, also Art. 26 E-VDSG, die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten untergraben, bspw. durch Bilden von Parallel- oder Untergesellschaften mit weniger als 250 Mitarbeitern, die dann ausschliesslich das Bearbeiten von besonders schützenswerten Personendaten sowie das Profiling übernehmen. Es stellt im Übrigen selbst für Einzelfirmen mit den heutigen wirklich einfachen Mitteln und Tools gar kein Problem oder überhaupt nennenswerten Mehraufwand dar, rechtsgenügliche und sichere Verzeichnisse der Bearbeitungstätigkeiten anzulegen bzw. zu führen. Nebenbei dient die Verzeichnispflicht der Bearbeitungstätigkeiten gerade kleinen Unternehmen dem Eigenschutz einschliesslich der notwendigen Sensibilisierung und Rechtssicherheit.

SWISS INSIGHTS

Swiss Data Insights Association

Swiss Insights, Swiss Data Insights Association, Gruebengasse 10, 6055 Alpnach

Per Email
fanny.matthey@bj.admin.ch
daniela.nueesch@bj.admin.ch

Alpnach, 6. Oktober 2021

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Matthey
Sehr geehrte Frau Nüesch
Sehr geehrte Damen und Herren

Swiss Insights, Swiss Data Insights Association vertritt die Interessen der Markt- und Sozialforschungsbranche. Viele unserer Mitglieder sind international tätige Unternehmen, welche sich bei der Bearbeitung von Personendaten regelmässig an die Vorgaben der EU-DSGVO zu halten haben. Für diese Unternehmen ist es zentral, dass das revidierte Schweizer Datenschutzgesetz auf den EU-Standard abgestimmt ist und keinen zusätzlichen Standard („*Swiss Finish*“) etabliert. Gerne nehmen wir zur eingangs genannten Sache wie folgt Stellung:

Am 25. September 2020 hat das Parlament – nach langen Debatten – die Totalrevision des Schweizer Datenschutzgesetzes (revDSG) verabschiedet. Dieses ist international abgestimmt, um dem EU-Standard (DSGVO) Rechnung zu tragen und enthält im Wesentlichen keine Swiss Finishes. Damit schafft das Gesetz Rechtssicherheit für Schweizer Unternehmen, welche sich (auch) an die Bestimmungen der DSGVO halten müssen. **Der Entwurf der Verordnung zum Datenschutzgesetz (E-VDSG) gefährdet die gewonnene Rechtssicherheit durch zahlreiche Regelungen, welche über diejenigen der DSGVO hinausgehen.** Wir bitten Sie, den Entwurf dahingehend zu überarbeiten, dass sämtliche Swiss Finishes und Widersprüche zum revDSG beseitigt werden. Die Verordnung hat sich auf Konkretisierungen des Gesetzes zu beschränken und darf insbesondere nicht Regelungen aufstellen, welche bewusst nicht in das Gesetz aufgenommen wurden (z.B. Art. 16 E-VDSG).

Unsere nachfolgenden Anregungen und Formulierungsvorschläge in Bezug auf einzelne Artikel des Entwurfs mögen Ihnen bei der Überarbeitung dienen. Alle aufgeführten Punkte sind aus unserer Sicht grundsätzlich zwingend zu berücksichtigen (Prio 1: rot, Prio 2: orange, Prio 3: gelb).

Bei allfälligen Rückfragen stehen wir Ihnen gerne zur Verfügung

Freundliche Grüsse

Stefan Langenauer
Präsident

Nicole Siegrist
Geschäftsführerin

Artikel	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag
Generell	Entgegen ihrer Natur als reine ***Ausführungs***verordnung zum Datenschutzgesetz enthält die E-VDSG Regelungen, welche über eine blosse Konkretisierung des revDSG hinausgehen.	Die VDSG hat ausschliesslich die Konkretisierung des revDSG zum Zweck (vgl. Erläuterungen, S. 9). Sie darf darüber hinaus keine zusätzlichen eigenen Regelungen vorsehen. Dies führte zu einer eigentlichen Parallelgesetzgebung.	Konsequente Streichung aller mit dem E-VDSG eingeführten **Swiss Finishes** (vgl. nachfolgend). Ergänzung der Titel in der Verordnung mit einer Verweisung auf die entsprechende gesetzliche Grundlage. Z.B.: „Art. 1 Grundsätze (Art. 8 Abs. 3 DSG)“
	Die zusätzlich aufgestellten Regelungen entbehren nicht nur einer Rechtsgrundlage im Gesetz, wo der Gesetzgeber teilweise bewusst anders entschieden hat, sondern gehen auch über das Niveau der DSGVO hinaus. Diese **Swiss Finishes** stehen aber im Widerspruch zur expliziten Zielsetzung des Gesetzgebers und auch des BJ, wonach Kompatibilität mit der DSGVO geschafft werden sollte (Erläuterungen, S. 10).	Wie das BJ in den Erläuterungen (S. 10) selbst ausführt, soll durch Kompatibilität mit der DSGVO Rechtssicherheit für Unternehmen geschaffen werden, welche sich an die DSGVO halten. Das gelingt freilich nicht, wenn die VDSG gegenüber dem revDSG (neue) **Swiss Finishes** einführt. Im Gegenteil, damit sind Doppelspurigkeiten und Widersprüche vorprogrammiert.	

1	Berücksichtigung des Implementierungsaufwands statt der -kosten als Kriterium aufnehmen.	Die Erläuterungen zur Berücksichtigung der Implementierungskosten als Kriterium bei der Beurteilung der Angemessenheit sind u.E. unpräzise (vgl. Erläuterungen, S. 16). Entgegen diesen Ausführungen sind die Implementierungskosten gemäss E-VDSG 1 I b bei der Beurteilung der Frage, ob eine Massnahme angemessen ist, zu berücksichtigen, und nicht erst, wenn es darum geht, sich für eine von mehreren angemessenen Massnahmen zu entscheiden. Zudem ist nicht allein auf die Implementierungs*kosten*, sondern generell auf den Implementierungs*aufwand* abzustellen. Das sollte in der Verordnung entsprechend präzisiert werden.	1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a.–c. […]; d. Implementierungs~~kosten~~*aufwand*. 2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen~~r~~ ~~Abständen~~ *Weise* zu überprüfen.
	Pflicht zur Überprüfung der Massnahmen in angemessener *Weise*	Die Massnahmen sind infolge risikobasierten Ansatzes nicht in angemessenen *Abständen*, sondern vielmehr in angemessener *Weise* zu überprüfen. Denn die Frage, ob eine Kontrolle nötig ist, hängt insbesondere davon ab, ob sich die Risiken geändert haben.	

3	Die Protokollierungspflicht nach VDSG 3 ist zu streichen.	Die Protokollierungspflicht nach VDSG 3 hat keine Grundlage im revDSG und widerspricht dem risikobasierten Ansatz. Auch „hohen" Risiken ist mit den im Einzelfall *adäquaten Massnahmen* zu begegnen. Die DSGVO sieht keine Protokollierungspflicht vor. Es handelt sich daher um einen **Swiss Finish**. Auf einer Dokumentationspflicht, wie sie im VE-DSG vorgesehen war, wurde aufgrund der Eingaben in der Vernehmlassung verzichtet bzw. sie wurde durch die Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen ersetzt. Diese geht weiter als die bisherige Pflicht zur Anmeldung der Datensammlung beim EDÖB. Es müssen neu alle Bearbeitungen in einem Verzeichnis aufgeführt sein. Es ist nicht erforderlich, an der Protokollierungspflicht festzuhalten, zumal diese in der Praxis mit hohen Zusatzkosten verbunden ist (insb. Software-Beschaffung etc.). Die Einführung der Protokollierungspflicht als Teil der Datensicherheit hätte stossende Auswirkungen: Falls trotz gegebenen Voraussetzungen keine DSFA durchgeführt wird, so hat dies gemäss revDSG *keine* Sanktion zur Folge. Wird hingegen eine DSFA durchgeführt, aber in der Folge gegen die allfällige Protokollierungspflicht (als Teil der Datensicherheit) verstossen, so ist das sanktionsbedroht. Der Verantwortliche hat die vorgängige Stellungnahme des EDÖB einzuholen, wenn sich aus der DSFA ergibt, dass eine geplante Bearbeitung trotz Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat. Der	**Streichung von VDSG 3**, zumindest für den Privatbereich.

		EDÖB kann dem Verantwortlichen bei etwaigen Einwänden (angemessene) ebenfalls Massnahmen vorschlagen.	
4	Die Pflicht zur Erstellung eines Reglements nach VDSG 4 ist zu streichen.	Die Pflicht zur Erstellung eines Reglements nach VDSG 4 I hat keine Grundlage im revDSG und widerspricht dem risikobasierten Ansatz. Auch „hohen" Risiken ist mit den im Einzelfall *adäquaten* Massnahmen zu begegnen. Die DSGVO sieht keine Pflicht zur Erstellung eines Reglements vor. Es handelt sich daher um einen **Swiss Finish**. Auf eine Dokumentationspflicht, wie sie im VE-DSG vorgesehen war, wurde aufgrund der Eingaben in der Vernehmlassung verzichtet bzw. sie wurde durch die Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen ersetzt. Diese geht weiter als die bisherige Pflicht zur Anmeldung der Datensammlung beim EDÖB. Es müssen neu alle Bearbeitungen in einem Verzeichnis aufgeführt sein. Es nicht erforderlich, an der praxisfernen Pflicht zur Erstellung eines Reglements festzuhalten.	**Streichung von VDSG 4**, zumindest für den Privatbereich.

6	Unklar, was die Ausführungen auf S. 24 der Erläuterungen zu den Anforderungen an den Inhalt des ADV gemäss Art. 22 Abs. 3 DSGVO bezwecken, zumal diese in Art. 6 E-VDSG nicht vorgesehen sind.	Diese Ausführungen suggerieren, dass der ADV gemäss VDSG 6 den inhaltlichen Anforderungen der DSGVO genügen müsse. Hierfür findet sich indes keine gesetzliche Grundlage. Auch die E-VDSG enthält keine inhaltlichen Vorgaben.	Klarstellung im Erläuterungsbericht, dass die VDSG – anders als die DSGVO – keinen Mindestinhalt an den ADV vorschreibt.
	Streichung der Pflicht zur Sicherstellung einer vertrags- oder gesetzesgemässen Bearbeitung.	„Sicherstellung" der vertrags- und gesetzesgemässen Bearbeitung ist nicht möglich. Analog DSGVO 28 I kann der Verantwortliche nur, aber immerhin verpflichtet werden, nur Auftragsbearbeiter zu beauftragten, welche durch angemessene Massnahmen die Bearbeitung im Einklang mit den Anforderungen des revDSG und den Schutz der Rechte der Betroffenen gewährleisten.	1 Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. ~~Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.~~ *Er arbeitet nur mit Auftragsbearbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen so durchgeführt werden, dass die Bearbeitung im Einklang mit den Anforderungen der Schweizer Datenschutzgesetzgebung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.* 2 ~~Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.~~ 3 Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich *oder in einer anderen Form, die den Nachweis durch Text ermöglicht,* genehmigt hat.
	Streichung von Abs. 2, weil der Auslandtransfer separat geregelt ist.	Abs. 2: Auslandtransfers sind separat geregelt (E-VDSG 8), weshalb für diese Regelung keine Notwendigkeit besteht. Sollte an dieser Regelung festgehalten werden, so wäre im letzten Satz zu präzisieren, dass „andernfalls ein geeigneter Datenschutz gemäss Art. 16 Abs. 2 revDSG zu gewährleisten ist."	
	Präzisierung des Begriffs „schriftlich", der auch „in Text nachweisbare Formen" umfasst.	Abs. 3: „Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	

10	Der Empfänger kann nicht verpflichtet werden, „die schweizerischen Datenschutzvorschriften“ einzuhalten. Das ist im Erläuterungsbericht klarzustellen.	Im Erläuterungsbericht (S. 28) ist festgehalten, dass der Empfänger verpflichtet werden müsse, „die schweizerischen Datenschutzvorschriften“ einzuhalten. Das ist unzutreffend; er muss die Standardklauseln einhalten, nicht jedoch Schweizer Datenschutzrecht. So verlangt auch E-VDSG 6 II, dass der Auftragsbearbeiter „gleichwertige“ Bestimmungen einhalten muss.	Klarstellung im Erläuterungsbericht, dass der Empfänger nicht verpflichtet werden muss, „die schweizerischen Datenschutzvorschriften“ einzuhalten.
	Ersatz des Begriffs „Sicherstellung“ durch „darauf hinwirken“.	Der Exporteur kann nicht „sicherstellen“, dass der Empfänger die Standarddatenschutzklauseln beachtet; er kann nur, aber immerhin darauf hinwirken.	1 Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um ~~sicherzustellen~~ *darauf hinzuwirken*, dass die Empfängerin oder der Empfänger diese beachtet. *Die Angemessenheit der Massnahmen richtet sich nach den Umständen im konkreten Fall und dem Stand der Technik.* 2 […]
	Präzisierung, dass sich die Angemessenheit der geforderten Massnahmen nach den Umständen im konkreten Einzelfall richte und die Anforderungen insb. dann höher seien, wenn es sich um besonders schützenswerte Personendaten handle.	Dies ist in den Erläuterungen (S. 28) unter Hinweis auf das BJ entsprechend festgehalten und sollte zur Klarstellung auch in die Verordnung einfliessen. Der risikobasierte Ansatz bei der Beurteilung von Datentransfers in Länder ohne angemessenen Datenschutz auf Grundlage der SCC ist zu bejahen. Allerdings ist dieser Ansatz mit Blick auf die Praxishinweise der EU-Behörden keinesfalls selbstverständlich. Entsprechend bedarf es einer Klarstellung in der Verordnung zur Schaffung von Rechtssicherheit.	
NEU	Präzisierung des räumlichen Anwendungsbereichs des revDSG (Auswirkungsprinzip, Art. 3 I):	Gemäss revDSG 3 I gilt das Gesetz für Sachverhalte, die sich in der Schweiz auswirken auch wenn sie im Ausland veranlasst werden. Weder das Gesetz noch die Verordnung halten fest, ob an die Auswirkungen weitere Anforderungen zu stellen sind. Eine solche qualifizierte Auswirkung (Spürbarkeit) ist erforderlich, um Übertreibungen bei der extraterritorialen Anwendung des Schweizer Datenschutzrechts vorzubeugen. Hierzu ist eine Regelung analog zum Marktortprinzip gemäss DSGVO aufzunehmen.	*Folgende Sachverhalte, die im Ausland veranlasst werden, wirken sich in der Schweiz aus:* *a. das Angebot von Waren oder Dienstleistungen gegenüber betroffenen Personen in der Schweiz;* b. *die Beobachtung des Verhaltens von betroffenen Personen, soweit ihr Verhalten in der Schweiz erfolgt.*

13	Richtigstellung, dass keine „Basisinformationen“ auf der ersten Kommunikationsstufe mitgeteilt werden müssen.	Das revDSG sieht nicht vor, dass die Betroffenen die „wichtigsten Informationen“ auf der „ersten Kommunikationsstufe“ erhalten müssen (vgl. aber Erläuterungen, S. 30). Vielmehr hält revDSG 19 I fest, die Information müsse „angemessen“ erfolgen. Daraus folgt, dass das die Mitteilung von den jeweiligen Umständen abhängig ist. Dabei sind auch Informationsinteresse und die Erwartungen des Betroffenen zu berücksichtigen: Während er damit rechnen mag, dass sich in einem Vertrag ein Hinweis auf den die Datenschutzerklärung findet, ist ein solcher auf Visitenkarten, E-Mails oder Briefpapier nicht üblich. Sollte sich eine Person dafür interessieren, kann ihr zugemutet werden, die Webseite des betreffenden Unternehmens zu konsultieren. Darum darf es nicht erforderlich sein, in Alltagssituationen – wie bei einer Terminvereinbarung, am Schalter – explizit auf die Datenschutzerklärung hinweisen zu müssen (s. Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 99). Zudem wäre ohnehin unklar, welches die „wichtigsten Informationen“ sind.	Richtigstellung im Erläuterungsbericht, dass den Betroffenen keine „Basisinformationen“ auf der ersten Kommunikationsstufe mitgeteilt werden müssen und dass auch das Informationsinteresse der Betroffenen im Einzelfall zu berücksichtigen ist.
	Keine Informationspflicht des Auftragsbearbeiters.	Der Auftragsbearbeiter hat gemäss revDSG keine Informationspflicht (vgl. revDSG 19). Eine solche kann nicht in der VDSG eingeführt werden.	**Streichung von Art. 13 VDSG**
	Unklare Anforderungen an Piktogramme.	Weil Piktogramme ohnehin nur ergänzend verwendet werden dürfen, sind daran keine zusätzlichen Anforderungen zu stellen. Zumal aufgrund der Erläuterungen nicht klar ist, was mit „maschinenlesbar“ gemeint ist.	
15	Die Informationspflicht bei der Bekanntgabe von Personendaten ist zu streichen.	Diese Informationspflicht entbehrt einer Grundlage im revDSG.	**Streichung von Art. 15**

		Auf die Richtlinie (EU) 2016/680 (Schengen-RL) ist für den Privatbereich nicht abzustellen. Die DSGVO sieht keine entsprechend Pflicht vor. Eine Umsetzung ist nicht erforderlich und schafft einen **Swiss Finish**. Der Auftragsbearbeiter ist gemäss revDSG wie bereits erwähnt nicht Adressat der Informationspflicht. Keine Notwendigkeit: Der Verantwortliche hat bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten.	
16	Die Informationspflicht über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten ist zu streichen.	Diese Informationspflicht entbehrt einer Grundlage im revDSG. Diese Pflicht wurde im Vorentwurf des DSG vorgeschlagen, im Rahmen der Vernehmlassung jedoch wieder gestrichen. Sie darf entsprechend nicht über die VDSG wieder eingeführt werden. Keine Notwendigkeit: Der Verantwortliche hat bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten.	**Streichung von Art. 16.**

18	Analog DSGVO 35 IV soll der EDÖB eine Liste erstellen und publizieren, welche Bearbeitungen enthält, für die eine bzw. keine DSFA zu erfolgen hat. Alternativ oder kumulativ sind Kriterien zu nennen, wonach ermittelt werden kann, ob eine DSFA durchzuführen ist oder nicht. „Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	Ohne Kriterien und/oder Liste mit Beispielen von Bearbeitungen, die eine DSFA erfordern bzw. nicht erfordern, besteht eine grosse Rechtsunsicherheit.	*1 Der Beauftragte erstellt eine Liste mit Bearbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Er kann zusätzlich eine Liste mit Bearbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.* *2* Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich *oder in einer anderen Form, die den Nachweis durch Text ermöglicht,* festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~
	Die Aufbewahrungsfrist ist zu streichen.	Die Dokumentationspflicht gemäss VDSG 18 entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Zudem besteht der Anreiz, der Dokumentationspflicht nicht nachzukommen, da diese – im Gegensatz zu einer Verletzung der Datensicherheit – nicht strafbar ist. Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelungen einen **Swiss Finish** darstellen.	
	Der Begriff der Schriftlichkeit ist zu präzisieren.	„Schriftlich" dürfte auch andere Formen erfassen, die den Nachweis durch Text ermöglicht (z.B. E-Mail). Das ist wie in andere Gesetzen (z.B. FIDLEG/FIDLEV) zu präzisieren.	

19	Die Auslegung des Begriffs „voraussichtlich“ ist falsch und zu korrigieren.	„Voraussichtlich“ heisst nicht, dass „in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen kann, eine Meldung erfolgen muss“ (so die Erläuterungen, S. 32). Der Begriff „voraussichtlich“ setzt vielmehr voraus, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko führt.	Richtigstellung im Erläuterungsbericht, dass in Fällen, wo das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, nicht gemeldet werden muss, sondern nur dann, wenn die Verletzung der Datensicherheit **höchstwahrscheinlich** zu einem hohen Risiko führt.
	Streichung der in der Verordnung gegenüber dem Gesetz zusätzlich eingeführten Mindestangaben bei einer Meldung einer Verletzung der Datensicherheit.	Gemäss revDSG 24 II hat der Verantwortliche in der Meldung einer Verletzung der Datensicherheit „mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen zu [nennen]“. Die E-VDSG sieht weitere Mindestangaben vor. Die DSGVO sieht keine Angabe von Zeitpunkt und Dauer der Verletzung vor. Es handelt sich daher um einen **Swiss Finish**.	1 Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit: a. die Art der Verletzung; ~~b. soweit möglich den Zeitpunkt und die Dauer;~~ ~~c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;~~ ~~d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;~~ e.-g. […] 2 […] *3* ~~Der~~ *Falls der* Verantwortliche *verpflichtet ist, die* ~~teilt den~~ betroffenen Personen *zu informieren, so teilt er ihnen* in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit. 4 […] ~~5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.~~
	Streichung der über das Gesetz hinausgehenden generellen Pflicht, die betroffene Person zu informieren.	E-VDSG 19 II geht über revDSG 20 IV hinaus. Während das Gesetz eine Information der betroffenen Person nur vorschreibt, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt, sieht die Verordnung vor, dass der Verantwortliche den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mitteilt.	
	Streichung der gesetzlich nicht vorgesehenen Dokumentationspflicht nach VDSG 19 V.	Dokumentationspflicht nach VDSG 19 V entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie nach der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor. Es handelt sich daher um einen **Swiss Finish**. Falls an der Dokumentationspflicht festgehalten werden sollte, ist zu präzisieren, dass nur meldepflichtige Verletzungen aufzubewahren sind.	

20	Die Auskunftserteilung sollte nicht nur schriftlich, sondern auch in einer anderen durch Text nachweisbaren Form möglich sein.	In den Erläuterungen (S. 34) wird festgehalten: „Es kann hier ferner präzisiert werden, dass zur schriftlichen Form auch die elektronische Form gehört." Diese Präzisierung ist in die Verordnung aufzunehmen.	1 […] 2 Die Auskunft wird in der Regel schriftlich *oder in einer Form, die den Nachweis durch Text ermöglicht,* erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat. 3-4 […] *5 Die betroffene Person hat keinen Anspruch auf Herausgabe von Dokumenten, selbst wenn diese Personendaten enthalten sollten.* ~~5 Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.~~
	Aufnahme der Präzisierung, dass der Begriff „Daten als solche" insbesondere auch eine Auskunft in aggregierter Form zulässt.	In den Erläuterungen (S. 35) wird ausgeführt: „Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Die mündliche Mitteilung von Informationen, zum Beispiel am Telefon, ist ebenfalls möglich, sofern die betroffene Person eingewilligt hat." Es besteht im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten bzw. Unterlagen. Vielmehr ist die Mitteilung nach entsprechender Debatte vom Gesetzgeber bewusst beschränkt worden auf die bearbeiteten Personendaten „als solche" (revDSG 25 II b). Damit soll namentlich auch die Auskunft in aggregierter Form ermöglicht werden. Dies sollte zwecks Präzisierung in der Verordnung verankert werden.	
	Dokumentationspflicht nach VDSG 20 V ist zu streichen.	Dokumentationspflicht nach VDSG 20 V entbehrt einer gesetzlichen Grundlage¨(vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch	

		die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen **Swiss Finish** darstellt. Die Regelung ist ferner unnötig, da aufgrund der Beweislast ohnehin im Interesse des Verantwortlichen mit Dokumentation den Nachweis erbringen zu können.	
22	Der Fristenbeginn ist zu präzisieren.	Präzisierung erforderlich: Wenn aus dem Auskunftsbegehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.	1 Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen. *Wenn aus dem Begehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst mit dieser Klarstellung zu laufen.* 2 […]

24	Klarstellung, dass „Datenportabilität“ kein Zwang zu standardisierten Datenbearbeitungssystemen beinhaltet.	Die „Datenportabilität“ wurde erst im Rahmen der parlamentarischen Debatte eingeführt. Entsprechend enthält die Botschaft keine Ausführungen dazu. Die Verordnung muss hier Konkretisierungsarbeit leisten.	*1 Das Recht der betroffenen Person, sie betreffende Personendaten vom Verantwortlichen heraus zu verlangen oder durch diesen an einen anderen Verantwortlichen übertragen zu lassen, begründet für den Verantwortlichen nicht die Pflicht, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten.* *2* […]
26	Es ist zu präzisieren, dass sich die allfällige Pflicht eines KMU zur Führung eines Verzeichnisses nicht auf sämtliche Bearbeitungen erstreckt, sondern auf diejenigen Bearbeitungen beschränkt ist, welche die Voraussetzung(en) triggern.	Der Bundesrat hat gemäss revDSG 12 V Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses vorzusehen für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und deren Datenbearbeitung ein „geringes Risiko“ mit sich bringt. Gemäss E-VDSG 26 bedeutet ein geringes Risiko, dass weder „umfangreich besonders schützenswerte Personendaten bearbeitet“ werden noch „ein Profiling mit hohem Risiko durchgeführt“ wird. Alle anderen Bearbeitungen bringen im Umkehrschluss ein geringes Risiko mit sich. Durch Präzisierung, dass sich die Pflicht zur Führung eines Verzeichnisses ausschliesslich auf diejenigen Bearbeitungen erstreckt, welche die Voraussetzung triggern, kann sowohl dem Schutz der betroffenen Personen als auch den Bedürfnissen der KMU angemessen Rechnung getragen werden (vgl. auch das Positionspapier des EDSA zu Art. 30 Abs. 5 DSGVO).	*1* Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. […] b. […] *2 Ist eine Voraussetzung nach Abs. 1 Bst. a und/oder b erfüllt, so ist die Verzeichnispflicht auf diejenige bzw. diejenigen Bearbeitungen beschränkt, welche dieser Voraussetzung bzw. diesen Voraussetzungen zugrunde liegen.* *3 Das Bearbeitungsverzeichnis ist schriftlich, oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu führen.*
	Es ist ferner zu präzisieren, dass das Verzeichnis nicht schriftlich, sondern auch in anderer Form, die den Nachweis durch Text ermöglicht, z.B. elektronisch, geführt werden kann.	Damit ist klargestellt, dass das Verzeichnis auch elektronisch geführt werden kann.	

***

SwissFoundations

association of swiss grant-making foundations
verband der schweizer förderstiftungen
association des fondations donatrices suisses
associazione delle fondazioni donatrici svizzere

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte I
Per E-Mail
jonas.amstutz@bj.admin.ch

Zürich/Genf, 7. Oktober 2021

Stellungnahme von SwissFoundations, dem Verband der Schweizer Förderstiftungen: Vernehmlassung zur Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren Bundesräte

Wir danken für die Möglichkeit, uns im Rahmen des Vernehmlassungsverfahrens zur VDSG äussern zu können und nehmen gerne wie folgt Stellung.

2001 gegründet, vertritt SwissFoundations als Verband der Schweizer Förderstiftungen über ein Drittel aller jährlichen Stiftungsausschüttungen in der Schweiz. Unsere Mitglieder und assoziierten Partner investieren jährlich mehr als CHF 1 Mrd. in gemeinnützige Projekte und Initiativen im In- und Ausland.

Chronologie

Das Parlament hat das neue Datenschutzgesetz (nDSG) beraten und am 25. September 2020 verabschiedet.

Am 23. Juni 2021 eröffnete der Bundesrat die Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz VDSG. Frist: 14. Oktober 2021.

Die liberalen Rahmenbedingungen in der Schweizer Gesetzgebung sind Grundlage für den Erfolg des Schweizer Stiftungsstandorts. Mit einem freiwillig gespendeten Stiftungsvermögen von CHF rund 100 Mrd. und über 13'000 gemeinnützigen Stiftungen gibt es in der Schweiz pro Kopf etwa sechsmal mehr gemeinnützige Stiftungen als in den USA oder Deutschland.

Als Stimme der Schweizer Förderstiftungen setzt sich SwissFoundations für den Schutz der Stifterfreiheit und die Modernisierung des Stiftungsstandortes ein. Philanthropisches Engagement erfordert Flexibilität, heute mehr denn je. Gesetzliche Regelungen tragen dazu bei, die Rahmenbedingungen für philanthropisches Handeln zu stärken oder zu schwächen und sind im Einzelfall entscheidend für die Wirksamkeit des Standorts. Wir wollen sicherstellen, dass gemeinnützige Mittel über Schweizer Stiftungen auch in Zukunft dem Allgemeinwohl zufliessen. So gilt es, gemeinnützigen Stiftungen, die zumeist Ihre Tätigkeit mit ehrenamtlichen Strukturen erfüllen, nicht mit unnötiger Bürokratie und weiteren Regulatorien zu belasten. Andernfalls laufen wir Gefahr, dass der immer grösser werdende Bürokratieaufwand den lebedigen Stiftungssektor in Schweiz dezimieren und zukünftige Stifter vom Stiften abhalten wird – zum Schaden der Allgemeinheit.

Das neue Datenschutzgesetz schafft einen enormen Verwaltungsaufwand und auch Stiftungen sind verpflichtet, die verschärften datenschutzrechtlichen Anforderungen umzusetzen.

Die bereits strengen Anforderungen des DSG dürfen durch die neue VDSG nicht noch weiter verschärft werden. Genau dies droht aber mit der neuen VDSG.

Insgesamt ist zu konstatieren, dass der Entwurf zum Teil unnötig weit über das Ziel bzw. über die gesetzlichen Vorgaben hinausschiesst.

So setzt beispielsweise Art. 2 des Verordnungsentwurfs die Vorgaben für die Datensicherheit hoch an, anstatt Mindestanforderung vorzugeben, wie in Art. 8 Abs. 3 DSG vorgesehen. Dies gilt es insbesondere auch in Hinblick auf kleinere gemeinnützige Organisationen mit ehrenamtlichen Strukturen zu vermeiden. Die Verordnung sollte von Organisationen aber nur verlangen, was diese realistischerweise erfüllen können. Kommt hinzu, dass ein Verstoss gegen die Mindestanforderungen an die Datensicherheit mit einer strafrechtlichen Busse bis zu CHF 250'000 geahndet wird (Art. 61 lit. c DSG).

Augenmass beweist der Entwurf hingegen bei der Ausnahmeregelung bezüglich der Pflicht zur Führung eines Datenbearbeitungsverzeichnisses von Art. 12 Abs. 5 DSG, Art. 26 Entwurf-VDSG. Der Entwurf anerkennt hier die Problematik der kleineren Unternehmen und anderer kleinerer privatrechtlicher Organisationen. SwissFoundations begrüsst die Ausnahmeregelung, wonach eine gesetzliche Pflicht zur Führung eines Datenbearbeitungsverzeichnis erst für Organisationen ab 250 Beschäftigten oder bei einer umfangreichen Bearbeitung besonders schützenswerter Personendaten bzw. bei einem Profiling mit hohem Risiko besteht.

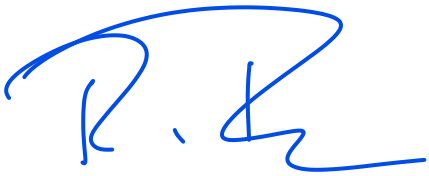
FAZIT

Zusätzliche Anforderungen und Bürokratie im Datenschutz durch die neue Verordnung zum Bundesgesetz über den Datenschutz (VDSG), die über die bereits strengen Vorgaben des neuen Datenschutzgesetzes hinausgehen, sind zu vermeiden. Dies gilt insbesondere in Hinblick auf kleinere gemeinnützige Organisationen mit ehrenamtlichen Strukturen.

Die Ausnahmeregel in Art. 26 Entwurf-VDSG beweisst Augenmass und wird von SwissFoundations begrüsst.

Wir bedanken uns für die Berücksichtigung unserer Stellungnahme und Anliegen und wünschen Ihnen eine konstruktive und zielführende Diskussion und Entscheidfindung.

Mit freundlichen Grüssen



Dr. Richard Brogle
Geschäftsführer SwissFoundations

Julia Jakob
SwissFoundations

SwissHoldings
Verband der Industrie- und Dienstleistungsunternehmen in der Schweiz

Nägeligasse 13
Postfach
CH-3001 Bern

+41 31 356 68 68
info@swissholdings.ch
www.swissholdings.ch

Frau Bundesrätin
Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
jonas.amstutz@bj.admin.ch

Bern, 14. Oktober 2021

Stellungnahme von SwissHoldings zur Revision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

SwissHoldings, der Verband der Industrie- und Dienstleitungskonzerne in der Schweiz, umfasst 60 der grössten Konzerne der Schweiz, welche zusammen rund 70% der gesamten Börsenkapitalisierung der SIX Swiss Exchange ausmachen. Gerne nehmen wir zur titelgenannten Vorlage wie folgt Stellung.

Wichtige zeitnahe umfassende Überarbeitung des Entwurfs entlang der nachfolgenden Grundsätze

Aus unserer Sicht ist es wichtig, dass die **Verordnung noch einmal wesentlich und zeitnah unter Einsetzung der notwenigen Ressourcen überarbeitet wird**. Folgende Punkte sind bei der Überarbeitung zu berücksichtigen:

1. **Es ist auf den Erhalt der Datenschutzäquivalenz zu achten. Dies ist eines der zentralen Anliegen unserer Mitgliedfirmen.** Der Erhalt der Datenschutzäquivalenz geht auch einher mit einer **zeitnahen Anpassung der Verordnung, die angesichts des aktuell grossen Anpassungsbedarfs am Entwurf auch eines allenfalls zusätzlichen Einsatzes der notwendigen Ressourcen bedarf.**

2. Weiter ist es in diesem Zusammenhang und auch selbststehend **zentral, dass die aktuell in der Vorlage enthaltenden zahlreichen Swiss Finishes, die über die Regelungen im EU-Raum hinausschiessen, aus der Vorlage eliminiert werden**. Das Parlament hat zu Recht bei der Beratung zum DSG im Wesentlichen auf die Swiss Finishes verzichtet. Diesem Grundsatz soll nun nicht durch die Verordnung widersprochen werden: Die Wirtschaft darf nicht durch übertriebenen Swiss Finish Bestimmungen mit unnötigem administrativem und finanziellem Aufwand belastet werden. Dies wäre überdies auch aus einer gesamtheitlichen Sicht kontraproduktiv, weil solche Schweizer Besonderheiten einen einheitlichen internationalen Datenraum verhindern und damit auch zulasten der Schweizer Unternehmen wettbewerbsverzerrend wirken.

3. Es muss – sei es betreffend die erwähnten Swiss Finishs, sei es bei allfälligen weiteren Einführungen unnötiger Hürden für die Unternehmen – darauf geachtet werden, dass der **Stossrichtung des revidierten DSG nicht widersprochen wird**. Dies gilt insbesondere für diejenigen Bestimmungen, die in der VDSG zu einem Swiss Finish führen, obwohl das revidierte DSG keinen solchen vorsieht, Dies gilt auch, wenn die VDSG unnötige Hürden für die Unternehmen vorsieht, die der Stossrichtung des revidierten DSG entgegenstehen. Es ist äusserst problematisch, wenn durch die Verordnung der Wille des Parlaments missachtet wird.

Wichtige konkrete Anpassungsvorschläge

Die im Vordergrund stehenden konkreten Anpassungsvorschläge in Zusammenhang mit diesen Grundsätzen sind den nachfolgenden Ausführungen zu entnehmen:

Art. 3 zur Protokollierungspflicht – ersatzlose Streichung:

Die Bestimmung stellt einen unnötigen Swiss Finish dar. Es gibt keine Berechtigung mehr für solche zusätzlichen Anforderungen unter dem neuen engmaschigen Regime des revidierten DSG. Das Parlament hat bewusst trotz detaillierter Formulierung der Anforderungen an die Datenschutzfolgenabschätzungen in Art. 22 nDSG auf eine Protokollierungspflicht verzichtet. Ferner würde die Einführung eine solche Pflicht auch gegen das im revidierten DSG verankerten Verhältnismässigkeitsprinzip verstossen.

Entsprechend ist der Artikel aus unserer Sicht ersatzlos zu streichen.

Art. 4 zum Bearbeitungsreglement von privaten Personen – ersatzlose Streichung:

Auch Art 4 stellt einen unnötigen Swiss Finish dar. Gleich wie für Art. 3 gilt, dass es keine Berechtigung mehr gibt für solche zusätzlichen Anforderungen unter dem neuen engmaschigen Regime des revidierten DSG. Zu beachten ist, dass die Abgrenzung zwischen dem Bearbeitungsreglement und den neuen Pflichten gemäss revidiertem DSG (Verzeichnis der Bearbeitungstätigkeiten, Art. 12 nDSG; Datenschutzfolgeabschätzung, Art. 22 nDSG) unklar und damit kontraproduktiv wäre. Ausserdem ist das Bearbeitungsreglement der VDSG

gerade ein Schulbeispiel für eine rechtliche Pflicht, die in der Praxis nicht gelebt und von der Behördenseite auch nicht vollzogen wurde. Hier bietet die Revision eine Chance, die VDSG an die Realität anzupassen und damit die VDSG zu stärken. Gesetze, die toter Buchstrabe sind bzw. nicht vollzogen werden, schwächen das Gesetz und damit den Rechtsstaat.

Art. 8 zur Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs – Notwendige Klarstellung, dass sich diese Bestimmung nur an den Bundesrat richtet:

Art. 8 in seiner jetzigen Formulierung könnte so verstanden werden, dass auch private Verarbeiter diese Beurteilung vornehmen müssen. Er richtet sich aber an den Bundesrat (s. Art. 16 des revidierten Datenschutzgesetzes). Dies muss im Artikel klargestellt werden.

Art. 13 zu den Modalitäten der Informationspflichten – Informationspflicht gegenüber betroffenen Personen nur für den Verantwortlichen und nicht für den Auftragsbearbeiter:

Die Bestimmung in ihrer aktuellen Formulierung steht im diametralen Widerspruch zur DSGVO (Art. 13 und 14 DSGVO) und stellt damit wiederum einen Swiss Finish dar. Auch widerspricht sie dem revidierten DSG (Art. 19 nDSG). In beiden Gesetzen trifft die Informationspflicht nur den Verantwortlichen.

Auch ist zu bemerken, dass diese Pflicht strafbewehrt ist (Art. 60n DSG). Dies führt dazu, dass auf diesem Weg auch die Strafbarkeit des Auftragsverarbeiters eingeführt würde. Hierfür bräuchte es aus rechtsstaatlichen Gründen ein Gesetz im formellen Sinn, was die VDSG nicht ist.

Entsprechend muss der Auftragsbearbeiter aus dem Titel des 2. Kapitals sowie aus Art. 13 gestrichen werden.

Art. 15 zur Information bei der Bekanntgabe von Personendaten – ersatzlose Streichung:

Auch bei diesem Artikel handelt es sich um einen unnötigen Swiss Finish. Die DSGVO sieht keine entsprechende Pflicht vor. Es gilt auch hier, dass es keine Berechtigung mehr gibt für solche zusätzlichen Anforderungen unter dem neuen engmaschigen Regime des revidierten DSG. Die Zusatzanforderungen in Art. 15 würden dazu führen, dass an übliche und vernünftige Kommunikationsmittel, selbst solche ohne erkennbare datenschutzrechtliche Risiken, völlig überrissene Anforderungen gestellt würden. Dies würde faktisch die Ver- oder Behinderung üblicher vernünftiger Kommunikationsmittel wie z.B. E-Mail bedeuten. Dies wiederum steht im Widerspruch zu den Zielen des Bundesrats, die Digitalisierung und Innovationskraft im Interesse des Wirtschaftsstandorts Schweiz zu fördern.

Entsprechend ist der Artikel ersatzlos zu streichen.

Art. 16 – ersatzlose Streichung oder zumindest wesentliche Anpassung des Artikels zu Informationen über die Berichtigung, Löschung oder Vernichtung sowie die Einschätzung der Bearbeitung von Personendaten:

Die Pflicht wurde im Rahmen der Vernehmlassung zum revidierten Datenschutzgesetz gestrichen und es ist entsprechend problematisch, wenn sie über die VDSG wieder eingeführt würde. Auch besteht keine Notwendigkeit, da ja der Verantwortliche bei der Datenbearbeitung ohnehin die Bearbeitungsgrundätze einzuhalten hat, ebenso wie die Empfänger von Personendaten.

Wird der Artikel nicht gestrichen, müsste aus dem Artikel zumindest das Wort «unverzüglich» gestrichen werden. Die analoge Bestimmung in der DSGVO (Art. 19) enthält denn auch keine solche Frist. Auch wäre es notwendig, dass im Artikel klargestellt würde, dass sich eine allfällige Pflicht nur auf die Bearbeitung von Personendaten bezieht, die auf entsprechende Begehren der betroffenen Person zurückgehen. Ohne die explizite Klarstellung kann diese Pflicht sonst so gelesen werden, dass sie auch anwendbar ist, wenn die Löschung etc. gar nicht auf ein entsprechendes Begehren der betroffenen Person zurückgeht. Das Gesetz sieht aber eine aktive Information über die Löschung nur vor, wenn ein entsprechendes Begehren vorliegt.

Art. 19. Abs. 5 und Art. 20 Abs. 5 betreffend Dokumentations- und Aufbewahrungspflicht – ersatzlose Streichung der Absätze:

Die Dokumentationspflicht dieser Absätze wurde nach der Vernehmlassung zum neuen Datenschutzgesetz durch die Pflicht zur Führung eines Verzeichnisses ersetzt; die DSGVO sieht keine Aufbewahrungspflicht vor, weshalb es sich auch hier wiederum um Swiss Finishes handelt.

Entsprechend sind diese Absätze ersatzlos zu streichen.

Wir danken Ihnen für die wohlwollende Prüfung unserer Anliegen und stehen bei allfälligen Fragen sehr gerne zur Verfügung.

Freundliche Grüsse

SwissHoldings
Geschäftsstelle

Dr. Gabriel Rumo
Direktor

Dr. Manuela Baeriswyl
Leiterin Recht

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin
Karin Keller-Sutter
Bundeshaus West, 3003 Bern

Einreichung per Mail an: jonas.amstutz@bj.admin.ch

Zürich, 13. Oktober 2021

Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Stellungnahme von swissICT zur laufenden Vernehmlassung

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zur «Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz» (VDSG) äussern zu können. Diese Gelegenheit nimmt der Verband swissICT gerne wahr.

Generelles Feedback

Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus. Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen. Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck.». Aus Sicht des einreichenden Verbands ist dieser Grundsatz in einigen Punkten der E-VDSG nicht eingehalten worden (vgl. beigefügte detaillierte Stellungnahme). Es ist zwingend, vor der Inkraftsetzung die Einhaltung dieses Grundsatzes in Bezug auf die einzelnen Vorschriften zu prüfen.

Unterstützung der Einreichungen von digitalswitzerland und der asut

Ergänzend zu unseren detaillierten Rückmeldungen im Anhang, unterstützen wir auch die Rückmeldungen von digitalswitzerland und der asut.

Über swissICT

swissICT ist der primäre Repräsentant des ICT-Werkplatzes Schweiz und der grösste Fachverband der Branche. swissICT verbindet über 2500 ICT-Unternehmen, Anwender-Unternehmen und Einzelpersonen. Der Verband fördert den Informationsaustausch, bündelt Bedürfnisse, publiziert die wichtigste Salärumfrage, formuliert ICT-Berufsbilder und ist Co-Veranstalter des wichtigsten Informatik- und Businesspreises «Digital Economy Award». swissICT ist zudem Co-Initiant der Zertifizierungsinitiative 3L Informatik zur Sicherstellung von Informatikkompetenz in der Arbeitswelt.

Wir danken Ihnen im Namen unserer Mitglieder im Voraus dafür, dass Sie unsere Anregungen in geeigneter Weise bei der weiteren Umsetzung berücksichtigen.

Gerne stehen wir Ihnen für Rückfragen und weitere Diskussionen zur Verfügung.

Freundliche Grüsse

Kathy Riklin
Vorstand swissICT
Alt-Nationalrätin
Leiterin swissICT Politikkommission

Christian Hunziker
Geschäftsführer swissICT
Delegierter des Verwaltungsrates 3L Informatik AG

Verordnung zum Bundesgesetz über den Datenschutz (VDSG) – Issue List

Vorbemerkungen:
Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus (Art. 164 Abs. 2 BV). Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen (Art. 182 Abs. 2 BV). Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die **Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck.**» (BGE 141 II 169, E. 3.3) Aus Sicht des einreichenden Verbands ist dieser Grundsatz in einigen Punkten der E-VDSG nicht eingehalten worden (vgl. nachfolgende Stellungnahme). Es ist zwingend, vor der Inkraftsetzung die Einhaltung dieses Grundsatzes in Bezug auf die einzelnen Vorschriften zu prüfen.

Allgemeine Bemerkungen (gesetzl. Grundlage, Kontext, Adäquanz: David)
1.Kapitel: Datensicherheit

Artikel / Absatz	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag	Bemerkungen
Art. 1 Grundsätze	Ergänzen	**Ad Art. 1 Abs. 1** Gemäss erläuterndem Bericht (vgl. Ziff. 4.1.1) wird richtigerweise nicht eine 100% Datensicherheit, sondern vielmehr das Einhalten der erforderlichen Sorgfalt verlangt. Folglich kann es sein, dass eine	1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessen	

		Verletzung der Datensicherheit stattgefunden hat, der datenschutzrechtliche Verantwortliche jedoch seine Sorgfaltspflichten und damit auch die Vorgaben von Art. 8 revDSG und Art. 1 E-VDSG eingehalten hat. Daraus ergibt sich, dass sich das Kriterium der Angemessenheit nicht auf die technischen/organisatorischen Massnahmen (TOM) sondern auf die angestrebte Datensicherheit (d.h. den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Personendaten vor Unbefugten) beziehen muss. Die einzusetzenden TOM müssen dagegen geeignet sein, um die angemessene Datensicherheit zu wahren. **Ad Art. 1 Abs. 1 lit. b** Es geht nicht um die Berücksichtigung der Risiken, sondern der *Rest*risiken nach den getroffenen Massnahmen. **Ad Art. 1 Abs. 1 lit. d** Die Aufführung der Implementierungskosten als vermeintliches Kriterium zur Beurteilung der Geeignetheit von TOM zur Wahrung einer angemessenen Datensicherheit ist unzutreffend, irreführend uns gehört gestrichen. Es suggeriert, dass auf den Einsatz einer TOM dann verzichtet werden dürfe, wenn sie zwar geeignet aber "zu teuer" wäre. In der Folge würde eine "günstigere", jedoch weniger geeignete TOM ausgewählt und umgesetzt, was aber aufgrund des Kostenkriteriums im Einklang mit Art.	sind, beurteilt sich nach den folgenden Kriterien: a. Zweck, Art, Umfang und Umstände der Datenbearbeitung; b. die verbleibende Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen (Restrisiko); c. der Stand der Technik; d. Implementierungsaufwand. 2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg angemessen zu überprüfen.	

		8 revDSG i.V.m. Art. 1 E-VDSG stehen würde. Dies ist jedoch sachlogisch unzutreffend und wird auch vom erläuternden Bericht verworfen. Dass der Verantwortliche aus einer Auswahl gleich geeigneter TOM diejenige auswählt, welche kostengünstiger ist, stellt eine betriebswirtschaftliche Selbstverständlichkeit dar und bedarf keiner (rein deklaratorischer) Erwähnung in einer Rechtsgrundlage. **Ad Art. 1 Abs. 2** Ob, wann und wie eine Überprüfung der TOM stattfinden soll, bestimmt sich nach zu schützenden Schutzziel sowie der TOM selber und muss durch den Verantwortlichen selber entschieden werden. Nur er ist in der Lage, den Besonderheiten des Einzelfalls hinreichend Rechnung zu tragen. Schliesslich ist die Fokussierung auf den zeitlichen Abstand einer Prüfung und zugleich das Vorsehen einer Prüfpflicht nicht sachgerecht, unnötig einengend und steht im Widerspruch zum risikobasierten Ansatz.		
Art. 2 Schutzziele	Ergänzen	S. oben für Begründung plus: Die aufgeführten Schutzziele sind nur einige von vielen Möglichkeiten, um eine angemessene Datensicherheit sicherzustellen. Es kann sehr wohl sein, dass aufgrund des individuellen Risikos auf die Sicherstellung einzelner oder theoretisch auch aller Schutzziele verzichtet wird und dennoch eine angemessene Datensicherheit gewährleistet werden kann.	Soweit geeignet, müssen die technischen und organisatorischen Massnahmen zur Gewährleistung der angemessenen Datensicherheit folgende Schutzziele anstreben:	

		Zusatz: Die Ziele ergeben sich aus den Bearbeitungsgrundsätzen/Gesetz und sind einzuhalten resp. anzustreben. Die Mittel zur Sicherstellung sind vielfältig und unterschiedlich. Die Zugriffskontrolle ist die Massnahme, wobei das Schutzziel der Zugriff ist.		
Art. 3 Abs. 1 Protokollierung	Ersetzen	Die Protokollierung ist eine mögliche technisch/organisatorische Massnahme (TOM) zur Gewährleistung einer angemessenen Datensicherheit. Beim Aufgreiffkriterium wurde ein Logikfehler begangen: Das verbleibende (hohe) Risiko für die Persönlichkeitsrechte als Ergebnis einer DSFA hat in der Regel nichts zu tun mit dem Risiko betreffend Datensicherheit. Ersteres besteht erfahrungsgemäss in der Nichteinhaltung von Bearbeitungsgrundsätzen wie z.B. der Transparenz, Datensparsamkeit, Zweckbindung oder Richtigkeit. Letzteres besteht dagegen in der Wahl nicht geeigneter TOM zur Gewährleistung der Vertraulichkeit, Integrität oder Verfügbarkeit. Folglich ist das Aufgreiffkriterium für die Protokollierung zur Gewährleistung einer angemessenen Datensicherheit anzupassen. Ferner ist die Protokollierung als TOM und Ausfluss des Grundsatzes von Privacy by Design und Default geeignet zur Wahrung einer Vielzahl von Bearbeitungsgrundsätzen und müsste anders verortet werden.	1 Ergibt sich im Einzelfall, dass für die Gewährleistung einer angemessenen Datensicherheit eine Protokollierung erforderlich ist, muss der private Verantwortliche und dessen Auftragsbearbeiter zumindest die Protokollierung folgender Vorgänge sicherstellen: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.	
Art. 3 Abs. 2	Streichen	Zu Abs. 2 (Bundesorgane): Die Bestimmung zur Protokollierung durch Bundesorgane ist unverhält-		

		nismässig und greift zu weit. Sie besteht unabhängig des Risikos und umfasst bspw. auch bereits das «Lesen». Ferner fehlt eine Definition zu «automatisierten Bearbeitungen». Wird die Bestimmung betreffend Protokollierung nicht ganz gestrichen (inkl, für Private), so ist die Bestimmung für Bundesorgane mindestens analog derjenigen für Private zu formulieren.		
Art. 3 Abs. 3	Ersetzen		3 Die Protokollierung hat Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist, zu geben.	
Art. 4 Bearbeitungsreglement von privaten Personen	Streichen	Das Bearbeitungsreglement ist eine mögliche organisatorische Massnahme zur Gewährleistung einer angemessenen Datensicherheit. Beim Aufgreiffkriterium wurde ein Logikfehler begangen: Auch hier werden erhöhte Risiken für Persönlichkeitsrechte (zu bejahen bei bes. schw. Personendaten und Profiling mit hohem Risiko) mit Aspekten der Datensicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) unzulässig vermengt. Folglich ist das Aufgreiffkriterium für das Bearbeitungsgreglement zur Gewährleistung einer angemessenen Datensicherheit anzupassen. Ferner ist das Bearbeitungsreglement als TOM und Ausfluss des Grundsatzes von Privacy by Design und		

		Default geeignet zur Wahrung einer Vielzahl von Bearbeitungsgrundsätzen und müsste anders verortet werden.		
Art. 5	Streichen	Es ist nicht ersichtlich, wieso zusätzlich zu den zu ergreifenden Massnahmen ein Bearbeitungsreglement implementiert werden soll. Die Instrumentarien der Datenschutz-Folgeabschätzung, der Bearbeitungsverzeichnisse sowie zur Gewährung der Datensicherheit die technischen und organisatorischen Massnahmen sind Instrumente, um den Schutz der Personendaten zu gewährleisten. Es ist nicht ersichtlich, inwiefern ein Reglement hier zusätzliche Sicherheit bieten soll. Zudem entbehrt die Bestimmung einer gesetzlichen Grundlage.		

2.Kapitel: Pflichten der Verantwortlichen und des Auftragsbearbeiters

Artikel / Absatz	**Kritikpunkt / Anregung / Änderungsvorschlag**	**Kurzbegründung**	**Formulierungsvorschlag**	**Bemerkungen**
Art. 6 Abs. 1	Beschränkung des Anwendungsbereichs	Art. 6 Absätze 1 und 2 sind Art. 22 VDSG nachempfunden, welcher aber ausschliesslich für Bundesorgane gilt (für Private galt bislang Art. 10a DSG ohne weitere Präzisierungen im VDSG). Es ist nicht einzusehen, weshalb diese beiden Absätze nun auf Private ausgeweitet wurden. Dies erscheint nicht erforderlich, ansonsten hätte man den entsprechenden Regelungsgehalt bereits in Art. 9 integrieren können (wenn er sowohl für Private als auch für Bundesorgane Geltung haben sollte).	1 ~~Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich.~~ Der Verantwortliche muss dafür Sorge tragen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.	

		Auch ist unklar, was «für den Datenschutz verantwortlich» heissen soll. Es fehlt auch eine gesetzliche Grundlage für den 2. Satz in Art. 6 Abs. 1.		
Art. 6 Abs. 2	Streichen	Art. 9 DSG regelt bereits, dass der Verantwortliche Daten nur so bearbeiten lassen darf, wie er es selbst darf. Es dürfte für den Verantwortlichen auch kaum möglich sein zu beurteilen, ob andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Allenfalls bezieht sich der Verfasser auf die Angemessenheit des Datenschutzes (was aber in Abschnitt 3, Ziff 8 geregelt wird). Ausserdem wird der Verantwortliche ohnehin in aller Regel den gleichwertigen Datenschutz auf vertraglichem Wege sicherstellen in Anlehnung an GDPR 28 Abs 4, und für Auftragsdatenbearbeiter ausserhalb der EU , z.B. über Standardvertragsklauseln des EDOEB. Das aber ist bereits in Art. 16 DSG abgedeckt.		
Art. 6 Abs. 3	Streichen	Art. 9 Abs. 3 DSG stellt bereit sicher, dass die Übertragung der Bearbeitung an einen Dritten nur mit vorgängiger Genehmigung des Verantwortlichen übertragen darf. Es ist nicht ersichtlich, warum hier beim Bund strengere Anforderungen (schriftliche Genehmigung) gelten sollen. Jedenfalls muss klargestellt werden, dass «schriftlich» soviel wie «in Textform» heisst und auch in allgemeiner Form erfolgen kann (analog der DSGVO).		
Art. 7	Streichen	Art. 24 DSG regelt die Meldung von Verletzungen der Datensicherheit. Es ist nicht ersichtlich, warum		

		hier für den Bund weitere Anforderungen auf Verordnungsstufe festgelegt werden. Die internen Prozesse sollten vom Bundesorgan selbst geregelt werden können. Zudem sieht bereits Art. 29 Abs. 1 E-VDSG eine Informationspflicht des Bundesorgans an den Datenschutzberater vor. Unklar ist ferner, was «Probleme» heissen soll.		

2.Kapitel, 2. Abschnitt: Bekanntgabe von Personendaten ins Ausland

Artikel / Absatz	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag	Bemerkungen
Art. 8 Abs. 1 lit. c	Teilweise Streichen	Die Berücksichtigung der Rechtsprechung würde dazu führen, dass die Beurteilung ständig überholt werden muss sobald irgendwo ein neuer Entscheid zum Datenschutz gefällt wird; das ist nicht praxisgerecht und schadet der Rechtssicherheit.	die geltende Gesetzgebung zum Datenschutz sowie deren Umsetzung ~~und die einschlägige Rechtsprechung~~	
Art. 8 Abs. 1 lit. e	Streichen	Kann das vom Bundesrat effektiv beurteilt werden? Wenn Art 8 lit e sinngemäss beibehalten wird, dann sollte sich die Formulierung an den Beurteilungskriterien der Europäischen Kommission orientieren.		
Art. 8 Abs. 4	Unpräzise Formulierung	Was bedeutet «bereits erfolgte Datenbekanntgaben»? Und gilt das auch, wenn ein geeigneter Datenschutz anderweitig gewährleistet ist? Falls diese Bestimmung auf Verantwortliche anwendbar ist, darf sie wirklich auf Verordnungsstufe stehen?		
Art. 9 Abs. 1	Fehlende Unterscheidung zwischen Anforderungen der Rollen der Exporteure und Importeure.	Wäre es nicht praktikabler – wenn der Wortlaut von Art. 9 gänzlich ersetzt wird und in Anlehnung an		

		Art. 28 Abs 4 GDPR einhergeht? In der Praxis müssen sich Schweizer ja ohnehin bereits an Art. 28 Abs 4 GDPR halten		
Art. 9 Abs. 1 lit. d und e	Beides streichen	Es fehlt eine gesetzliche Grundlage für die Vorgabe, die Länder oder Organisationen zu nennen, in die Daten weiterübermittelt werden (falls das hier überhaupt gemeint ist).		
Art. 9 Abs. 1 lit. f	Streichen	Diese Anforderungen sind in der Verhältnismässigkeit nach lit. a bereits enthalten.		
Art. 9 Abs. 1 lit. g	Präzisieren	Relevant sind nur die Empfänger, die den Vertrag schliessen.	g. die Empfängerinnen und Empfänger;	
Art. 9 Abs. 1 lit. j	Streichen	Siehe die allgemeine Anmerkung zu Art. 9 Abs. 1 (fehlende Unterscheidung nach den Rollen der Parteien).		
Art. 9 Abs. 1 lit. k	Streichen	Es sollte in Klammern jeweils auf die Bestimmung im DSG verwiesen werden, wo dieses Recht der betroffenen Person geregelt ist. Bei Bekanntgaben im Rahmen einer Auftragsbearbeitung ist dies nicht legitim. Siehe die allgemeine Anmerkung zu Art. 9 Abs. 1 (fehlende Unterscheidung nach den Rollen der Parteien).		
Art. 10 Abs. 1	Streichen oder mit Vorschlag ersetzen.	Der Verantwortliche kann prinzipiell nicht sicherstellen, dass der Empfänger die Klauseln beachtet, aber er kann und muss sich vergewissern, z.B. durch Audits, denn der Verantwortliche haftet ja ohnehin für die Verarbeitung der Personendaten durch den Auftragsbearbeiter.	1 Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um dazu beizutragen, dass die Empfängerin oder der Empfänger diese beachtet.	

Art. 13 Abs. 1	Die Regelungen in Kapitel 2 sollten mit GDPR einhergehen, damit Private in der Praxis einheitliche Prozesse aufstellen können.	Der Auftragsbearbeiter hat **keine Pflicht zur Information über die Beschaffung von Personendaten,** diese trifft den Verantwortlichen. Zudem ist der Verantwortliche nicht zu einer «Mitteilung» verpflichtet, sondern zur Bereitstellung der Information. Ein Zugangsprinzip gilt nicht. Die Erläuterungen können so gelesen werden, dass eine Information über eine Website nicht genügt. Das ist praxisfremd und hat im Gesetz keine Grundlage. Es sollte festgehalten werden, dass die Information über eine Website genügt, wie es auch der allgemeinen Praxis entspricht.	Der Verantwortliche ~~und der Auftragsbearbeiter teilent die Information~~ informiert über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form.	
Art.13 Abs. 2	Streichen	Es ist kein Ziel des Datenschutzes, verschiedene Dokumente zu vergleichen, wie es der Erläuterungsbericht als Ziel aufführt. Es fehlt zudem eine gesetzliche Grundlage für die Anforderungen an Piktogramme nach Art. 13 Abs. 2, und es fehlen auch allgemein akzeptierte Standards für die Maschinenlesbarkeit von Piktogrammen.		
Art. 14	Streichen	Wird hier nicht vermischt zwischen Datenschutz und gesetzlichen Mitwirkungspflichten? Der Datenschutz ist ja unabhängig davon relevant, ob Informationen freiwillig oder zwingend erteilt werden müssen. Ein Hinweis auf Freiwilligkeit ist nicht erforderlich, wenn diese aus dem Umständen hervorgeht.		
Art. 15	Streichen	Der Auftragsbearbeiter ist gemäss Art. 19 DSG nicht informationspflichtig, eine solche Pflicht kann		

		nicht auf Verordnungsstufe eingeführt werden. Auch kennt der Auftragsbearbeiter die Angaben gar nicht, über die er hier informieren soll. Zudem ist auch nicht ersichtlich, wie und warum der Verantwortliche die Empfängerinnen und Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit informieren sollte. Die Pflicht zur Richtigkeit ergibt sich ja aus dem DSG, es braucht keine zusätzlichen Massnahmen auf Verordnungsstufe, und es wäre auch völlig praxisfremd, vom Verantwortlichen zu verlangen, in jeder E-Mail an einen Dritten auf die Datenqualität hinzuweisen.		
Art. 16	Streichen	Inwiefern könnte die Benachrichtigung unmöglich sein? Diese Regelung war im Vorentwurf des DSG vorgesehen, wurde aber gestrichen. Es widerspricht daher dem Willen des Parlaments, wenn eine solche Regelung nun in der VDSG wieder eingeführt würde. Zudem wird die «Einschränkung» der Bearbeitung erwähnt. Dieses Betroffenenrecht gibt es in der DSGVO, aber nicht im (rev)DSG.		
Art. 17	Streichen	Eine solche Bestimmung ist überflüssig, aber auch missbrauchsanfällig. Wenn der Verantwortliche eine automatisierte Entscheidung nach der Anhörung nicht ändert, wird man ihm vorwerfen, dies sei eine gezielte Benachteiligung.		
Art. 18	Präzisieren	Es gibt keine gesetzliche Grundlage für eine Aufbewahrung in «Schriftform», wenn damit nicht soviel wie «in Textform» gemeint ist. Auch für die Auf-	Der Verantwortliche muss die Datenschutz-Folgenabschätzung in Textform festhalten.	

		bewahrungspflicht fehlt eine Grundlage. Wenn Aufbewahrung, dann in einer adäquaten nachvollziehbaren Form. Zudem werden Folgenabschätzungen im Lauf der Zeit ggf. angepasst. Widerspräche dies der Aufbewahrung der ersten Fassung? Das Aufbewahrungserfordernis wirft mehr Probleme auf, als es lösen könnte.		
Art. 19 Abs. 1 lit. e	Angleichen	Angleichung an Art. 24 Abs. 1 und 2 DSG, wo die Risiken genau spezifiziert sind. Zudem kann es nur um hohe Risiken für die Betroffenen gehen, denn andernfalls besteht gar keine Meldepflicht gegenüber dem EDÖB.	die Folgen, von denen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen ausgehen;	
Art. 19 Abs. 1 lit. f	Ergänzen	Es sollten auch Massnahmen getroffen werden, um die Risiken zu vermeiden. Auch wenn ein Mangel behoben ist sollten trotzdem gleichzeitig Folgen bzw. Schäden gemildert werden (Schadenminderungspflicht).	welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben, die Risiken zu vermeiden und/oder die Folgen zu mildern;	
Art. 19 Abs. 3	Ergänzen	Art. 24 Abs. 4 und 5 DSG sieht vor, dass eine Information an die betroffenen Personen nur unter bestimmten Voraussetzungen erfolgen muss. Die Kontaktperson gegenüber dem EDÖB wird gerade bei grösseren Unternehmen sicherlich nicht ein und dieselbe Person sein, die sich um Anfragen von betroffenen Personen kümmert. Vielmehr müsste dann auch eine generische Inbox für Datenschutzanfragen möglich sein.	Der Verantwortliche teilt den betroffenen Personen im Anwendungsbereich von Art. 24 Abs. 4 und 5 DSG in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e und f mit.	
Art. 19 Abs. 5	Streichen	Die Dokumentation erfolgt bereits im Rahmen der Meldepflicht gemäss Art. 24 DSG. Eine weitere Dokumentationspflicht ergibt sich aus dem DSG nicht,		

		hat also keine gesetzliche Grundlage, und ist auch nicht geboten. Wer hat Abschluss des Meldeverfahrens noch ein Interesse an einer Dokumentation und warum soll diese genau 3 Jahre aufbewahrt werden?		

3.Kapitel: Reche der betroffenen Person

Artikel / Absatz	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag	Bemerkungen
Art. 20 Abs. 1	Keine explizite Erwähnung des Auskunftsbegehrens und der Auskunftserteilung "auf elektronischem Wege".	Bisher wurde explizit festgehalten, dass Auskunftsbegehren sowie die Auskunftserteilung auf elektronischem Weg erfolgen könnten. Dies fehlt nun gänzlich, allerdings wurde in der Erläuterung festgehalten, dass dies die elektronische Form beinhalte. Dennoch ist die fehlende ausdrückliche Erwähnung ein Anachronismus und dient nicht der Klarheit.	Das Auskunftsbegehren wird schriftlich oder auf elektronischem Weg gestellt. Die Auskunft wird in der Regel schriftlich oder auf elektronischem Weg erteilt.	
Art. 20 Abs. 2	Fehlende Erwähnung des Kopierrechts	Wie bis anhin kann die Einsichtnahme vor Ort erfolgen. Gemäss Erläuterung haben die Betroffenen das Recht, Fotokopien von bestimmten Akten im Dossier zu machen. Zudem ist unklar, weshalb nur von "bestimmten" Akten Kopien gemacht werden dürfen.	Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen.	
Art. 20 Abs. 3	Kritik am Adressatenkreis	Ob die Auskunft "verständlich" ist, hängt immer vom Empfängerhorizont ab. Es sollte indessen nicht so sein, dass der Verantwortliche bei gewissen Empfängern umfassendere Angaben, Zusatzangaben oder Erläuterungen machen muss. Dieser	Die Auskunft muss ~~für betroffene Person~~ verständlich sein.	

		Pflicht sollten somit gewisse Grenzen gesetzt werden.		
Art. 20 Abs. 5	Streichen	Es fehlt eine gesetzliche Grundlage für eine solche Dokumentations- und Auskunftspflicht. Die Dokumentation erfolgt i.d.R. ohnehin durch das Antwortschreiben an den Betroffenen.		
Art. 21 Abs. 2	Streichen	Die Bestimmung sieht die Weiterleitung des Begehrens an den Auftragsbearbeiter vor. Dies ist einerseits selbstverständlich, andererseits aber missverständlich, da der falsche Eindruck entsteht, der Verantwortliche sei mit der Weiterleitung seiner Auskunftspflicht nachgekommen, was Art. 25 Abs. 4 revDSG widerspricht.		
Art. 22	Ergänzen	Dies räumt dem Verantwortlichen einen sehr grossen Spielraum ein und es sollte eine Maximalfrist festgelegt werden.	Kann die Auskunft nicht innert 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber benachrichtigen und ihr die Frist mitteilen, in der die Auskunft erfolgen wird.	
Art. 23 Abs. 1	Präzisieren	Eine Kostenbeteiligung kann verlangt werden, wenn die Auskunftserteilung mit einem "unverhältnismässigen Aufwand" verbunden ist. Was darunter zu verstehen ist und wozu der Aufwand in Relation gesetzt werden soll, bleibt jedoch unklar, so dass die Anwendungsfälle dieser Bestimmung sehr offen und unklar sind.	Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. Ein solcher liegt u.a. vor, wenn [...]	
Art. 23 Abs. 3	Präzisieren	Der Fristbeginn ist zu präzisieren.	Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu	

			setzen und kann ihr Gesuch innert zehn Tagen seit Mitteilung zurückziehen.	
Art. 24	Widersprüchliche Regelung	Art. 21-23 der Verordnung sollen auf das Recht auf Datenherausgabe und -übertragung sinngemäss anwendbar sein. Damit findet die für Auskunftsbegehren gemäss Art. 25 Abs. 7 revDSG geltende Frist von 30 Tagen qua Art. 22 der Verordnung auch auf Begehren auf Datenherausgabe und -übertragung Anwendung, obwohl das revDSG dies nicht vorsieht. Dadurch wird einerseits ein Widerspruch zum revDSG geschaffen; andererseits fragt sich, ob eine solche Frist durch den Verordnungsstatt den Gesetzgeber einzuführen ist.	Die Artikel 20 Absätze 1, 4 und 5, sowie 21~~, 22~~ und 23 sind auf das Recht auf Datenherausgabe und -übertragung sowie deren Einschränkungen sinngemäss anwendbar.	

4.Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Artikel / Absatz	**Kritikpunkt / Anregung / Änderungsvorschlag**	**Kurzbegründung**	**Formulierungsvorschlag**	**Bemerkungen**
Art. 25 Abs. 1 lit. a Datenschutzberaterin oder Datenschutzberater	Streichen Hinweis: Diskrepanz zwischen Art. 10 revDSG und Art. 25 E-VDSG.	Diese lit. a ist zu weitgehend: Der/die Datenschutzberater/-in kann als Anlaufstelle wirken, aber keine allgemeinen Überwachungspflicht wahrnehmen. Diese lit. a ist deshalb ersatzlos zu streichen. Diese Bestimmung ist zudem ein nicht stufengerechter Eingriff in die Privatrechtsautonomie bzw. stellt eine Verletzung aufsichtsrechtlicher Vorgaben zahlreicher regulierter Branchen mit hoher Arbeitsteilung dar (vgl. z.B. FINMA-RS 2017/01 Corporate Governance Banken).		

		Weil Datenschutz eine typische Querschnittsmaterie mit einer sehr hohen Arbeitsteilung, unter Einbezug zahlreicher Experten aus unterschiedlichen Bereichen, darstellt, kann sie nicht von einer einzigen Funktion ausgeübt werden. Alles andere wäre ein krasses Übernahmeverschulden, dass zahlreiche auch arbeits- und vertragsrechtliche Sorgfaltspflichtsverletzungen nach sich ziehen würde. Ferner verletzt diese Bestimmung das weltweit als Standard etablierte drei Linien Verteidigungsmodel in dem es die Erkennung, Einhaltung und Korrektur von datenschutzrechtlichen Vorgaben einer einzelnen Funktion, namentlich dem Datenschutzberater, auferlegt.		
Art. 25 Abs. 1 lit. b	Streichen	Der Zugang hat zwingend im Zusammenhang mit den Aufgaben der/ des Datenschutzberaters/-in zu stehen. Die vorgeschlagene Formulierung ist zu weitgehend.		
Art. 26	Ablehnung eines konkreten Stichtags.	In Bezug auf die Mitarbeiteranzahl sollte auf eine durchschnittliche Stellenprozentzahl pro Jahr abgestellt werden.	Unternehmen und andere privatrechtliche Organisationen, die ~~am Anfang eines Jahres~~ durchschnittlich im vergangenen Jahr weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, (…)	

5.Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane

Artikel / Absatz	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag	Bemerkungen
Art. 28 Abs. 2 lit. a Anforderungen und Aufgaben	Streichen	Dieser Abs. 2 lit. a ist zu weitgehend: Der/die Datenschutzberater/-in kann als Anlaufstelle wirken, aber keine allgemeinen Überwachungspflicht wahrnehmen. (Vgl. dazu auch Kommentare zu Art. 25 E-VDSG).	2 Sie oder er muss folgende Aufgaben wahrnehmen: (…) Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass die rechtlichen Datenschutzvorschriften formell verletzt wurden	
Art. 29	Präzisieren	Der Zugang hat zwingend im Zusammenhang mit den Aufgaben der/ des Datenschutzberaters/-in zu stehen. Die vorgeschlagene Formulierung ist zu weitgehend.	Zugang zu allen Auskünften, Unterlagen, Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren, die im Zusammenhang mit der Tätigkeit des/der Datenschutzberater/-in stehen und sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.	
Art. 31	Ergänzen	Grundsätzlich ist die automatisierte Bearbeitung von Personendaten heute bereits etabliert: Eine so generelle Bewilligungspflicht von Projekten kann nicht im Sinne des Gesetzgebers sein: Grundsätzlich bestehen gesetzliche Grundlagen und gesetzliche Bearbeitungspflichten, so dass zusätzliche Kriterien für die Bewilligungspflicht	Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von besonders schützenswerten Perso-	

		zu implementieren sind, wie dies in Art. 35 revDSG geregelt ist. Art. 35 Abs. 1 DSG bezieht die Bewilligungspflicht nur auf die automatisierte Bearbeitung von besonders schützenswerten Personendaten. Dies ist im Verordnungsentwurf zu ergänzen. Diese Bestimmung kann so nicht auch für externe Bundesorgane wie Pensionskassen etc. gelten, da für diese u.U. spezialrechtliche Geheimhaltungspflichten gelten.	nendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden	
Art. 32	Streichen	Dass bereits geplante und unabhängig des (potenziell) hohen Risikos jede automatisierte Bearbeitung gemeldet werden muss, führt zu einem unverhältnismässigen Mehraufwand. Auch liegen die verlangten Informationen im Zeitpunkt der Projektfreigabe häufig noch nicht vor. Ganz generell fehlt es aber an einer gesetzlichen Grundlage zur Meldung geplanter Datensammlung an den EDÖB und der Zusatznutzen für die Persönlichkeitsrechte ist nicht ersichtlich.		
Art. 33	Ergänzen	Die Neuerungen, die die Bewilligungspflicht auslöst, muss einen signifikanten Impact auf die zu bearbeitenden besonders schützenswerten Personendaten haben. Nicht jedes Pilotprojekt i.S. des DSG darf bewilligungspflichtig werden – das würde Innovation hemmen.	Eine Testphase als Pilotversuch ist unentbehrlich, wenn eine der folgenden Bedingungen erfüllt ist und die geplante Bearbeitung von besonders schützenswerten Personendaten einen signifikanten Einfluss hat auf letztere:	

		Es ist nicht ersichtlich, wieso lit. c notwendig ist. Abrufverfahren ist nur eine mögliche Konstellation, die zu prüfen ist.		
Art. 34	Ersetzen	Es wird nicht festgelegt, was bei Nichteinhaltung des DSG droht resp., wenn es zu Änderungen kommt, die z.B. einen Entzug der Bewilligung zur Folge haben könnte. Wann liegt eine solche Konstellation vor? Fristen? Verfahren? Wieso ist in lit. d von Sicherheits- und Datenschutzmassnahmen die Rede und nicht von technischen und organisatorischen Massnahmen?	Lit. d eine Beschreibung der ~~Sicherheits- und Datenschutzmassnahmen~~technischen und organisatorischen Massnahmen;	
Art. 34 lit. e	Streichen	Es ist wohl nicht in jeder Konstellation ein Verordnungsentwurf nötig – dies scheint so nicht sinnvoll zu sein.		
Art. 34 lit. f	--	Es ist unklar, ob in jedem Fall ein Antrag zu Handen des Bundesrats nötig ist.		
Art. 35	--	Es ist festzuhalten, dass der Bericht für weitere Schritte beigezogen werden muss.		

Artikel / Absatz	**Kritikpunkt / Anregung / Änderungsvorschlag**	**Kurzbegründung**	**Formulierungsvorschlag**	**Bemerkungen**
Art. 36	Streichen	Diese Bestimmung macht im Lichte von Art. 39 DSG keinen Sinn. Art. 39 gilt ja ohnehin nur für die Bearbeitung für nicht personenbezogene Zwecke durch Bundesorgane, die Forschung, Planung oder Statistik betreiben. Solche Bundesorgane sollten dann nicht noch unterscheiden müssen, ob jetzt eine Bearbeitung für Forschung, Planung oder Statistik eventuell doch noch eine personenbezogene Komponente hat.		

6.Kapitel: EDÖB

Artikel / Absatz	Kritikpunkt / Anregung / Änderungsvorschlag	Kurzbegründung	Formulierungsvorschlag	Bemerkungen
37	--	--	--	--
38	--	--	--	--
39 Abs. 1	--	--	--	--
39 Abs. 2	Satz 1 eleganter formulieren. Zusätzlich mit einem Satz 2 ergänzen.	Die Bundesorgane können die datenschutzrechtliche Relevanz nicht unbedingt stets abschätzen. Es könnte daher etwas übersehen werden.	Satz 1: Die Bundesorgane legen dem EDÖB alle Rechtsetzungsentwürfe vor, die die Bearbeitung von Personendaten, den Datenschutz sowie den Zugang zu amtlichen Dokumenten betreffen. Satz 2: Der EDÖB kann überdies von den Bundesorgane selbständig das Vorlegen von Rechtsetzungsentwürfen, die nach seiner Auffassung die Bearbeitung von Personendaten, den Datenschutz sowie den Zugang zu amtlichen Dokumenten betreffen, verlangen.	--
40	--	--	--	--
41 Abs. 1	--	--	--	--

41 Abs. 2	Satz 1 eleganter formulieren.	--	Er sieht interne Prozesse vor, die gewährleisten, dass die Bearbeitungen gemäss dem Bearbeitungsreglement vorgenommen werden.	--
42	--	--	--	--
43	--	--	--	--
44	--	--	--	--
45	--	--	--	--

7.Kapitel: Schlussbestimmungen

Artikel / Absatz	**Kritikpunkt / Anregung / Änderungsvorschlag**	**Kurzbegründung**	**Formulierungsvorschlag**	**Bemerkungen**
46	--	--	--	--
47	--	--	--	--
48	--	--	--	--

Association SWISSPRIVACY
info@swissprivacy.law

Département fédéral de justice et police
Palais fédéral ouest
3003 Berne
Par courriel à :
Jonas.amstutz@bj.admin.ch

Lausanne, le 12 octobre 2021

Projet de révision totale de l'ordonnance relative à la Loi fédérale sur la protection des données

Madame la Conseillère fédérale,
Mesdames, Messieurs,

Dans le délai imparti au 14 octobre 2021, l'association SWISSPRIVACY a le plaisir de participer spontanément à la consultation du projet de révision totale de l'ordonnance relative à la nouvelle Loi fédérale du 25 septembre 2020 sur la protection des données[1].

Chapitre 1 Dispositions générales
Les art. 1 à 12 P-OLPD contiennent des dispositions générales relatives aux art. 1 à 18 nLPD. À ce sujet, les remarques suivantes peuvent être émises.

Corolaire du principe de sécurité de l'art. 8 nLPD, les art. 1 à 5 P-OLPD prescrivent les exigences minimales en matière de sécurité que tout responsable du traitement doit respecter. Le responsable du traitement qui ne respecte pas ces exigences minimales réalise une infraction pénale, passible d'une amende dont le plafond est fixé à CHF 250'000.– (art. 61 let. c nLPD). Or le P-OLPD ne définit pas avec la précision nécessaire les mesures techniques et organisationnelles à mettre en œuvre dont la violation aurait pour effet de faire entrer en jeu la responsabilité pénale du responsable du traitement. Il apparaît ce faisant contraire au principe de légalité auquel le droit pénal obéit (art. 1 CP).

Les conditions relatives à l'obligation de journalisation prévue à l'art. 3 P-OLPD diffèrent selon si le responsable du traitement est une personne privée ou un organe fédéral. Dans le premier cas, l'obligation de journalisation s'applique en cas de risque résiduel élevé (art. 3 al. 1 P-OLPD), alors que dans le second cas, l'obligation de journalisation s'applique en cas de traitement automatisé (art. 3 al. 2 P-OLPD). Cette distinction ne doit pas être maintenue dans la version finale de l'OLPD. L'obligation de journalisation doit être limitée aux cas représentant un risque résiduel élevé.

Les art. 6 et 7 P-OLPD précisent les prescriptions légales quant à la sous-traitance de données personnelles ancrée à l'art. 9 nLPD. L'art. 6 al. 2 P-OLPD dispose que, lorsqu'un sous-traitant n'est pas soumis à la nLPD, le responsable du traitement s'assure que d'autres dispositions légales garantissent une protection équivalente. Cette disposition nous interpelle dès lors que le champ d'application territorial tel que fixé à l'art. 3 nLPD repose sur le critère des effets, celui-ci étant relativement large. Dès lors que le sous-traitant d'un responsable du traitement traite *de facto* des données personnelles de personnes résidant en Suisse, nous ne voyons pas dans quel cas un sous-traitant n'est pas soumis à la nLPD. Nous recommandons ainsi sa suppression. Par ailleurs, l'art. 6 al. 3 P-OLPD oblige l'organe fédéral, en sa qualité de responsable du traitement, d'approuver par écrit la sous-traitance de deuxième rang. Selon nous, seuls les organes fédéraux soumis à la Directive (UE) 2016/680[2] devraient être soumis à cette obligation.

[1] nLPD ; FF 2020 7397.
[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Les art. 8 à 12 P-OLPD précisent les prescriptions légales liées à la communication de données personnelles à l'étranger des art. 16 à 18 nLPD. L'art. 8 P-OLPD diffère de l'art. 16 nLPD en ce sens qu'il prévoit en plus de l'État et de l'organisme international qu'un territoire ou une section déterminée dans un État peut se voir considérer comme ayant un niveau de protection adéquat. Cette précision nous surprend, dès lors que la nLPD ne le prévoit pas à proprement parler, raison pour laquelle nous recommandons sa suppression. En ce qui concerne le respect des droits humains, ce critère n'est pas pertinent et devrait également être supprimé. Finalement, nous soulignons que la procédure d'évaluation n'est pas réglée, en particulier le processus selon lequel un État pourrait demander une décision d'adéquation et si celle-ci est sujette à recours. Il convient ainsi de préciser ces éléments.

Nous relevons à ce stade que le P-OLPD ne précise pas l'art. 14 nLPD relatif au représentant, disposition ajoutée par l'Assemblée fédérale. À ce sujet, il nous semble utile de préciser dans la version finale de l'OLPD l'absence de responsabilité subsidiaire du représentant, qui pourrait notamment découler de l'obligation de tenir un registre. Les modalités de sa désignation et de ses connaissances doivent également être précisées, à l'instar de celles concernant le conseiller à la protection des données.

Chapitre 2 Obligations du responsable du traitement et du sous-traitant
Les art. 13 à 19 P-OLPD complètent les art. 19 à 24 nLPD relatifs aux obligations du responsable du traitement et du sous-traitant. Plusieurs dispositions nous interpellent.

L'art. 14 P-OLPD prévoit une disposition particulière relative au devoir d'informer des organes fédéraux lors de la collecte des données personnelles. Cette disposition ne nous semble pas nécessaire, dès lors que le caractère facultatif doit être indiqué dans tous les cas et pas uniquement en cas de recours à un questionnaire.

L'art. 16 P-OLPD prévoit que le responsable du traitement informe sans délai les destinataires auxquels il a communiqué des données personnelles de la rectification, de l'effacement ou de la destruction, ainsi que de la limitation du traitement des données personnelles. Selon nous, les obligations fondées sur l'art. 16 P-OLPD devraient être limitées dans le temps. Il devrait en outre être précisé que ces obligations ne fondent pas un devoir pour le responsable du traitement de conserver une copie des données communiquées et des destinataires y relatifs.

L'art. 18 P-OLPD prévoit que le responsable du traitement consigne par écrit l'analyse d'impact relative à la protection des données personnelles, en tous les cas pendant deux ans après la fin du traitement des données. Imposer la forme écrite ne nous semble pas justifié et l'analyse d'impact relative à la protection des données devrait pouvoir être établie et conservée sous forme électronique. Bien qu'il découle du Rapport explicatif relatif à la procédure de consultation que la forme écrite comprend la forme électronique (cf. p. 24), il nous paraît essentiel de rappeler que la forme écrite exige une signature (TAF A-3548/2018 du 19 mars 2019, consid. 4.8.4). Dès lors, si la forme écrite devait être maintenue, elle doit être comprise de manière plus large que la règle formelle des art. 12 ss CO. Ce point doit être spécifiquement prévu (il en va de même en ce qui concerne l'art. 20 P-OLPD). En outre, il nous semble que le recours à la notion de « traitement » pourrait conduire à une conservation relativement longue, dès lors qu'il est admis que l'archivage de données est un traitement (art. 5 let. d nLPD).

L'art. 19 P-OLPD prévoit les modalités liées à l'annonce des violations de la sécurité des données et concrétise l'art. 24 nLPD. Afin de gagner en précision, l'al. 1 pourrait préciser que cet alinéa s'applique « en cas d'annonce obligatoire de violations de la sécurité des données », et non lors de toute violation. Le responsable du traitement qui voudrait informer le PFPDT de manière volontaire ne devrait ainsi pas forcément donner toutes les informations listées à l'al. 1. Concernant la notification échelonnée, elle est bienvenue. Il pourrait cela étant être utile de préciser si cela constitue bel et bien une possibilité (« peut » ; *kann*), et non une obligation (à l'instar de l'art. 33 par. 4 RGPD[3], malgré le texte imprécis qui semble indiquer une simple possibilité). Enfin, alors que la nLPD ne prévoit pas de telle obligation, nous sommes étonnés de découvrir une obligation, reprise du droit de l'Union européenne, de documenter les violations (al. 5). Cette obligation, qui ne découle pas d'une délégation législative, n'est pas valable et donc inefficace. Elle devrait ainsi être supprimée. Elle est en outre imprécise, car il n'est pas clair, comme pour l'al. 1, si, aux yeux de l'Office fédéral de la justice, cette obligation aurait dû viser toutes

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

les violations (comme à l'art. 33 par. 5 RGPD) ou uniquement celles qui doivent être annoncées au PFPDT.

Chapitre 3 Droits de la personne concernée
Les art. 20 à 24 P-OLPD complètent les art. 25 à 29 nLPD relatifs aux droits des personnes concernées. Nous relevons ce qui suit.

Les art. 20 ss P-OLPD concernent les modalités liées au droit d'accès. L'art. 20 al. 1 P-OLPD, ainsi que l'art. 20 al. 2 P-OLPD précisent que la demande de renseignement peut être faite par écrit (sauf exception), de même que l'envoi des renseignements. En lien avec notre commentaire relatif à l'analyse d'impact relatif à la protection des données, l'exigence de la forme écrite (et des règles formelles qui en découlent) ne se justifie pas. La forme électronique, et ses exigences, doivent être expressément prévues. En outre, l'art. 20 al. 2 P-OLPD dispose que d'entente avec le responsable du traitement, ou sur sa proposition, la personne concernée peut consulter ses données sur place. Selon nous, la consultation sur place doit pouvoir avoir lieu indépendamment de savoir qui l'a proposée. L'art. 20 al. 5 P-OLPD prévoit que le responsable du traitement documente le motif pour lequel il refuse, restreint ou diffère la communication des informations. Ce devoir de documentation ne découle pas de la nLPD et pourrait sortir du cadre des art. 25 ss nLPD. Finalement, la terminologie (« informations », « renseignements ») pourrait être uniformisée.

L'art. 22 al. 1 P-OLPD dispose que les renseignements, ou les causes de la restriction, sont fournis dans les 30 jours suivants réception de la demande. Il semble important de préciser que ce délai de 30 jours court dès la réception de la demande ou de la confirmation de l'acceptation des frais. À ce sujet, l'art. 23 al. 3 P-OLPD prévoit que la personne concernée doit être préalablement informée du montant des frais et se voir la possibilité de retirer sa requête dans les dix jours. La personne concernée ne devrait pas seulement pouvoir retirer sa demande, mais il devrait également être prévu qu'elle puisse confirmer sa demande en acceptant les frais potentiels. Dans la pratique, l'absence de réponse est problématique puisque le responsable du traitement doit déployer des efforts disproportionnés sans obtenir de garantie quant au paiement. Toutefois, il serait contraire à l'essence du droit d'accès de subordonner le paiement des frais à l'envoi des informations.

L'art. 12 al. 5 nLPD dispose que « [l]e Conseil fédéral prévoit des exceptions pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées ». La concrétisation de cette délégation expresse reste trop vague et manque le but d'atteindre une certaine sécurité juridique. Le rapport explicatif mentionne pourtant un « catalogue » (p. 12), que l'on peine à retrouver à l'art. 26 P-OLPD.

Chapitre 4 Dispositions particulières pour le traitement de données personnelles par des personnes privées
Les art. 27 à 45 P-OLPD contiennent des dispositions particulières pour le traitement de données personnelles par des organes fédéraux et complètent les art. 33 à 59 nLPD. Nous relevons à ce propos ce qui suit.

L'art. 42 P-OLPD prévoit que le PFPDT peut transmettre les informations relatives à l'annonce d'une violation de la sécurité des données au NCSC afin qu'il analyse l'incident. La personne responsable de l'annonce doit toutefois donner son accord. La notion de « responsable du traitement » devrait être favorisée à celle de « personne responsable de l'annonce », qui se rapproche de la notion de personne tenue d'annoncer de l'art. 24 al. 6 nLPD.

Veuillez croire, Madame la Conseillère fédérale, Mesdames, Messieurs, à l'expression de notre parfaite considération.

Le Comité de l'association SWISSPRIVACY

swissstaffing

Per E-Mail an:

jonas.amstutz@bj.admin.ch

Herr
Jonas Amstutz
Bundesrain 20
3003 Bern

Dübendorf, 14. Oktober 2021

Vernehmlassungsantwort: Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrte Damen und Herren

Gerne äussern wir uns im Rahmen der oben genannten Vernehmlassung innert Frist zum Verordnungsentwurf zum Bundesgesetz über den Datenschutz. Einleitend werden wir unsere grundlegenden Bemerkungen darlegen. In der Folge werden wir zu einzelnen Artikeln Kommentierungen vornehmen und jeweils konkrete Änderungsanträge stellen.

swissstaffing ist das Kompetenz- und Servicezentrum der Schweizer Personaldienstleister. Als Arbeitgeberverband vertritt swissstaffing die Anliegen seiner rund 430 Mitglieder gegenüber Politik, Wirtschaft und Gesellschaft. Swissstaffing fördert die Interessen der Personal-dienstleistungs-Branche und setzt sich aktiv für das Image der Temporärarbeit ein.

Grundsätzliche Bemerkungen:

- Die E-VDSG enthält entgegen ihrer Natur als reine Ausführungsverordnung zum revDSG mehrere Bestimmungen, welche über eine blosse Konkretisierung des revDSG hinausgehen. Der Sinn und Zweck von Ausführungsverordnungen beschränkt sich darauf, die Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Keinesfalls darf eine Ausführungsverordnung zu einer eigentlichen Parallelgesetzgebung führen.
- Den von der E-VDSG zusätzlich aufgestellten Bestimmungen fehlt es nicht nur an einer Rechtsgrundlage im revDSG. Sie gehen teilweise sogar weiter als die Bestimmungen in der europäischen Datenschutzgrundverordnung (DSGVO).
- Es wäre praktisch, bei den Verordnungsbestimmungen jeweils auf denjenigen Artikel der revDSG zu verweisen, um dessen Konkretisierung es geht.
- Wir erachten es als notwendig, den Unternehmen eine angemessene Frist für die Umsetzungsarbeiten einzuräumen. Insbesondere für die Erstellung von Verzeichnissen und - sofern darauf entgegen unserem Antrag (vgl. hiernach zu Art. 4) nicht verzichtet wird – von Bearbeitungsreglementen braucht es Übergangsfristen.

swissstaffing

Zu den einzelnen Artikeln der E-VDSG

Art. 1 Grundsätze
Absatz 1: *Art. 1 lit. d nennt die «Implementierungskosten» als Angemessenheitskriterium für die Datensicherheit.*
Hier sollte nebst den geldwerten Umsetzungsaufwendungen auch der Arbeitsaufwand mitberücksichtigt werden.

Antrag: Wir beantragen den Begriff «**Implementierungsaufwand**» anstatt «Implementierungskosten» zu verwenden.

Absatz 2: *Dieser Absatz verlangt, dass die Massnahmen über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen sind.*
Eine Überprüfung macht jedoch vor allem dann Sinn, wenn es wirklich zu relevanten Veränderungen eines Risikos kommt. Somit ist es nicht zweckmässig, die Überprüfung ausschliesslich von zeitlichen Aspekten abhängig zu machen. Wir erachten eine Überprüfung in «angemessener Weise» als zielführender.

Antrag: Wir beantragen eine Pflicht zur Überprüfung der Massnahmen in **angemessener Weise** anstatt in angemessenen Abständen.

Art. 2 Schutzziele
Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen….

Der Terminus «erreichen» ist unseres Erachtens zu absolut. Eine absolute Datensicherheit kann nicht erfüllt werden. Möglich ist es lediglich, diese anzustreben.

Antrag: Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele **anstreben**.

Art. 3 Protokollierung
Der in Art. 3 statuierten *Protokollierungspflicht* fehlt es an einer Rechtsgrundlage im revDSG. Selbst die DSGVO sieht eine solche Protokollierungspflicht nicht vor.

Antrag: Die Protokollierungspflicht im Sinne von Art. 3 E-VDSG ist zu streichen.

Art. 4 Bearbeitungsreglement von privaten Personen
Art. 4 Abs. 1 verlangt, dass Private ein Reglement erstellen, wenn sie a) umfangreiche besonders schützenswerte Personendaten bearbeiten oder b) ein Profiling mit hohem Risiko durchführen.

Die Pflicht betreffend Erstellung eines Reglements hat im revDSG keine Rechtsgrundlage. Auch Art. 8 revDSG kann nicht als Rechtsgrundlage dienen, da dieser Artikel lediglich die Datensicherheit im engeren Sinne regelt. Überdies sieht auch die DSGVO keine Pflicht zur Erstellung eines Reglements vor.

Antrag: Die Pflicht zur Erstellung eines Bearbeitungsreglements gemäss Art. 4 E-VDSG ist zu streichen.

Art. 6 Modalitäten
Art. 6 Abs. 1 statuiert die Pflicht, für den Verantwortlichen, die vertrags- und gesetzesmässige Bearbeitung durch den Auftragsbearbeiter «sicherzustellen».

Die Formulierung «Sicherstellung» der vertrags- und gesetzesgemässen Bearbeitung impliziert, dass eine solche «Sicherstellung» möglich ist, was jedoch nicht zutrifft. Der Verantwortliche kann nur, aber immerhin, dafür Sorge tragen, dass das revDSG eingehalten wird.

Gemäss Art. 9 Abs. 2 revDSG muss sich der Verantwortliche vergewissern, dass die Datenbearbeitung korrekt erfolgt. Unseres Erachtens bietet sich hier eine solche Formulierung an.

Antrag zu Art. 6 Abs. 1: Streichung des Terminus «Sicherstellung» und Ersatz durch eine weniger verpflichtende Formulierung wie bspw.: «Der Verantwortliche vergewissert sich, dass die Daten vertrags- und gesetzesgemäss bearbeitet werden.

Die Vorschrift von ***Art. 6 Abs. 2,*** *wonach der Verantwortliche sich vergewissern muss, dass andere Bestimmungen einen gleichwertigen Datenschutz gewährleisten, sofern der Auftragsbearbeiter nicht dem DSG untersteht*, macht für uns deshalb wenig Sinn, weil bereits Art. 16 und 17 revDSG die Thematik abdecken**.**

Antrag zu Art. 6 Abs. 2: Streichung von Art. 6 Abs. 2 E-VDSG.

Art. 9 Datenschutzklauseln und spezifische Garantien
Gemäss Art. 9 Abs. 2 E-VDSG muss der Verantwortliche in angemessener Weise Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.

Eine solche «Sicherstellung» ist nicht möglich. Der Begriff «Sicherstellung» suggeriert zu Unrecht, dass es eine Garantie für die Einhaltung der Klauseln gibt.

Antrag zu Art. 9 Abs. 2: Der Terminus «sicherstellen» sollte ersetzt werden, (bspw.) durch die Formulierung «darauf hinwirken».

Art. 10 Standarddatenschutzklauseln
Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Art. 16 Abs. 2 lit. d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.
Hier gelten die zu Art. 9 Abs. 2 E-VDSG gemachten Ausführungen analog.

Antrag: Der Terminus «sicherstellen» sollte ersetzt werden, (bspw.) durch die Formulierung «darauf hinwirken».

Art. 13 Modalitäten der Informationspflichten
Art. 19 revDSG sieht nur für den Verantwortlichen, nicht aber für den Auftragsbearbeiter, eine Informationspflicht vor. Mangels gesetzlicher Grundlage im revDSG kann eine solche Pflicht daher auch nicht in der E-VDSG statuiert werden.

Antrag zu Art. 13 Abs. 1: Der Auftragsbearbeiter ist aus der Bestimmung zu streichen.

Art. 15 Information bei der Bekanntgabe von Personendaten
Gemäss Art. 15 E-VDSG informieren der Verantwortliche und der Auftragsbearbeiter die Empfängerin bzw. den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.
Diese Regelung entbehrt einer gesetzlichen Grundlage in der revDSG. Es kommt hinzu, dass der Auftragsbearbeiter gemäss revDSG nicht informationspflichtig ist (vgl. die Ausführungen hiervor zu Art. 13 E-VDSG).

Antrag: Art. 15 E-VDSG streichen.

Art. 16 Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten
Die unter diesem Titel statuierten Informationspflichten entbehren einer gesetzlichen Grundlage und sind daher zu streichen.

Antrag: Art. 16 E-VDSG streichen.

Art. 18 Form und Aufbewahrung der Datenschutz-Folgenabschätzung
Art. 18 E-VDSG schreibt eine zweijährige Aufbewahrungsfrist nach Beendigung der Datenbearbeitung vor. Für eine solche Aufbewahrungsfrist fehlt es in der revDSG an einer gesetzlichen Grundlage. Das revDSG enthält abgesehen vom Verzeichnis keine Dokumentationspflichten. Auch die DSGVO sieht keine Aufbewahrungspflicht vor.

Antrag: Der Passus «Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.» ist zu streichen.

Art. 19 Meldung von Verletzungen der Datensicherheit
Eine Dokumentations- und Aufbewahrungspflicht wie sie Art. 19 Abs. 5 E-VDSG vorsieht, kennt das revDSG nicht. Daher können entsprechende Pflichten mangels gesetzlicher Grundlage auch nicht via Verordnung eingeführt werden.

Antrag: Streichung von Art. 19 Abs. 5 E-VDSG.

swissstaffing

Art. 20 Modalitäten des Auskunftsrechts
Gemäss Art. 20 Abs. 1 E-VDSG wird das Auskunftsbegehren schriftlich gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden.
In der heutigen Zeit der fortgeschrittenen Digitalisierung muss präzisiert werden, dass auch die elektronische Form ohne Einschränkung zugelassen ist.

Antrag zu Art. 20 Abs. 1: Wir schlagen vor, dass die Auskunft ermöglicht wird, sofern ein Begehren schriftlich oder in einer anderen durch Text nachweisbaren Form gestellt wird.

Art. 20 Abs. 5 E-VDSG sieht eine Aufbewahrungspflicht der Dokumentation von mindestens drei Jahren vor. Mangels einer gesetzlichen Grundlage für diese Pflicht im revDSG ist diese Bestimmung zu streichen.

Antrag: Streichung von Art. 20 Abs. 5 E-VDSG.

Art. 23 Ausnahmen von der Kostenlosigkeit
Die gemäss Art. 23 Abs. 2 statuierte Kostenbeteiligung von maximal CHF 300.00 ist angesichts der Kosten, welches ein Auskunftsbegehren verursachen kann, klar zu tief.
Hier ist der Vergleich zur DSGVO angebracht, welche keine betragsmässige Höchstgrenze kennt, sondern auf die «Angemessenheit» abstellt.
Der Höchstbetrag ist daher auch in der E-VDSG angemessen zu erhöhen.

Antrag: Angemessene Erhöhung des Maximalbeitrags an der Kostenbeteiligung für ein Auskunftsbegehren (mindestens CHF 1'000.--).

Art. 26 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten
Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet oder b. Es wird ein Profiling mit hohem Risiko durchgeführt.

Unklar ist, was unter «umfangreich besonders schützenswerten Personendaten» zu verstehen ist. Dies sollte genauer definiert werden, andernfalls Rechtsunsicherheit besteht.

Zu präzisieren ist unseres Erachtens zudem, wie die 250 Mitarbeitenden zu zählen sind. Sind hier auch Teilzeitstellen miterfasst?

Antrag: Der Begriff Mitarbeitende ist durch «Vollzeitstellen» zu ersetzen. Der Begriff «umfangreich besonders schützenswerten Personendaten» ist genauer zu definieren.

Inkraftsetzung und Übergangsbestimmungen
Die Totalrevision des Datenschutzrechtsrechts bringt gewichtige Änderungen mit sich und hat weitreichende neue Verpflichtungen für die Unternehmen zur Folge. Eine angemessene Umsetzungsfrist ist notwendig, zumal im neuen DSG keine Übergangsfristen vorgesehen sind und sowohl das totalrevidierte DSG als auch die totalrevidierte Verordnung bei Inkrafttreten bereits vollständig implementiert sein sollten.

Insbesondere die Erstellung von Verzeichnissen und Bearbeitungsreglementen (sofern darauf entgegen unserem Antrag nicht verzichtet wird) bedarf einer Übergangsfrist.

Für die Umsetzungsarbeiten in den Unternehmen erachten wir einen Zeitraum von einem Jahr, laufend ab Inkraftsetzung des revidierten Gesetzes / Verordnung, als zweckmässig und notwendig.

Wir bedanken uns für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anliegen.

Bei allfälligen Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

M. Fischer-Rosinger

Myra Fischer-Rosinger
Direktorin

Boris Eicher
Leiter Rechtsdienst

Thurbo AG, Postfach, CH-8280 Kreuzlingen 1

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz BJ
Bundesrain 20
3003 Bern

per e-Mail

Kreuzlingen,
13. Oktober 2021 - JCT

Telefon (direkt)
+41 71 554 00 35

E-Mail
jean-christophe.thieke@thurbo.ch

Stellungnahme zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

Für die Möglichkeit, im Rahmen der Vernehmlassung über die Revision der Datenschutzverordnung (VDSG) Stellung nehmen zu können, danken wir Ihnen.

Die Regionalbahn Thurbo AG ist ein Unternehmen der SBB mit Beteiligung des Kantons Thurgau und ist mit eigener Konzession im regionalen Personenverkehr in der Ostschweiz tätig. Mit über 25 Mio. Reisenden pro Jahr und über 490 Mitarbeitenden prägen wir den öffentlichen Verkehr in der Ostschweiz massgeblich, einfach, persönlich und fokussiert. Dabei denkt und arbeitet Thurbo nachhaltig und versteht sich als sicherer, verlässlicher Partner für Kundinnen und Kunden sowie die öffentliche Hand. Die Sicherheit sowie der Schutz der Daten und der Persönlichkeitsrechte der Kundinnen und Kunden sowie der Mitarbeitenden geniesst für die Thurbo AG daher Priorität.

Als Tochterunternehmung der SBB und im Verbund des öffentlichen Verkehrs in der Alliance SwissPass gelten bei uns bereits hohe Standards im Datenschutz. Die Thurbo AG betreibt keine eigenen Verkaufskanäle für Billette und Abonnemente, sondern bezieht diese Leistungen bei der SBB oder anderen öV-Partnerunternehmungen. Personenbezogene Daten verarbeitet die Thurbo AG als Arbeitgeberin, klar reglementiert im Umfeld von Marketing und Kundeninformation sowie in grösserem Umfang bei der Feststellung, Erfassung, Bearbeitung und im Inkasso von Reisen ohne gültigen Fahrausweis.

Für die Stellungnahme zur Revision der Datenschutzverordnung schliesst sich die Thurbo AG vollumfänglich den Stellungnahmen der SBB AG vom 12. Oktober 2021 sowie des Verbandes öffentlicher Verkehr (VöV) vom 4. Oktober 2021 an. Als regionaler öV-Anbieter mit mittelständisch geprägten Strukturen möchten wir, auch mit Blick auf die Vielzahl der kleinen und mittleren Unternehmen im öffentlichen Verkehr, nochmals explizit auf bestimmte kritische Punkte hinweisen:

Im Rahmen der hängigen RPV-Reform sind Änderungen des Personenbeförderungsgesetzes (PBG) im Artikel 54 vorgesehen. Im Zusammenhang mit dem erst nach Vernehmlassung zur RPV-Reform

revidierten DSG und der geplanten VDSG verstehen wir die Bestimmungen des PBG so, dass Transportunternehmungen in der konzessionierten Personenbeförderung den datenschutzrechtlichen Regelungen für Bundesorgane unterstehen würden.

Dies steht unseres Erachtens nicht nur im Widerspruch mit der aktuellen Rechtsprechung (Urteil A-5921/2020 des Bundesverwaltungsgerichtes vom 29. Juli 2021), sondern dürfte für betroffene Kundinnen und Kunden erhebliche Erschwernisse zur Folge haben, besonders im Vorfeld wie auch im Nachgang von Reisen im öffentlichen Verkehr:

Insbesondere im Service-après-Vente (Kundenservice per Telefon oder per Mail) oder bei Reisen ohne gültigen Fahrausweis, wenn es darum geht, kundenorientierte Lösungen zu finden, hätte die Anwendung der datenschutzrechtlichen Regelungen für Bundesorgane grosse Auswirkungen: Abläufe, Ausweis- und Dokumentationspflichten würden weder von Kundinnen und Kunden akzeptiert, noch wären sie für Transportunternehmungen wirtschaftlich zu erbringen. Auswirkungen auf Billettpreise oder den Abgeltungsbedarf der öffentlichen Hand sowie im Falle von Reisen ohne gültigen Fahrausweis auf die Höhe von Gebühren wären nicht ausgeschlossen.

Die Thurbo AG kontrolliert in ihren Zügen die Billettgültigkeit bei über 1.6 Millionen Reisenden pro Jahr und hält hierbei bei etwa 25.000 Reisenden pro Jahr festgestellte Sachverhalte und Personendaten bei Reisen fest, für die kein gültiges oder nur ein teilgültiges Billett vorgewiesen werden konnte.

Die Anwendung der datenschutzrechtlichen Bestimmungen für Bundesorgane sowie der einschlägigen Vorgaben des DSG und der geplanten VDSG könnte nach unserem Dafürhalten beispielsweise bedingen, dass die Transportunternehmungen mit ihrem Kontrollpersonal im Zug in die Lage versetzt und verpflichtet werden müssten, stets die Richtigkeit der erfassten Personalien zu prüfen, das Recht auf Nachweis der Personalien im Zweifel durchzusetzen und Angaben in der Nachbearbeitung proaktiv auf ihre Richtigkeit zu überprüfen. Dies ist rechtlich (u.a. keine Ausweispflicht in der Schweiz) wie auch praktisch nicht umsetzbar.

Die Menge erfasster Daten, die hohe Vergleichbarkeit der Fallmuster und der Einnahmeausfall je Einzelfall bedingt darüber hinaus zwingend eine automatisierte Weiterverarbeitung von Fall-/Personendaten aus der Kontrolltätigkeit bis hin zum Mahnwesen. Dabei sind Prozesse und Speicherung von Daten bereits heute darauf ausgelegt, eine möglichst schlanke, aber datenschutzkonforme Datenhaltung zu gewährleisten, mit der auch den Anforderungen an eine sachlich und zeitlich begrenzte Rückverfolgbarkeit von Verstössen gegen die Billettpflicht gemäss PBG entsprochen wird.

Weiterentwicklungen im privatrechtlich ausgerichteten öV-Tarifangebot bzw. öV-Vorschriften, Erfahrungen mit Praxisfällen und die wirtschaftlich ausgerichtete Verbesserung von Abläufen im Unternehmen erfordern zudem eine stetige Weiterentwicklung der Bearbeitungsverfahren. Dies würde durch die Anwendung der datenschutzrechtlichen Vorgaben für Bundesorgane im Vergleich zu Unternehmen, welche den Datenschutzbestimmungen für private Personen unterstehen, erheblich gehemmt.

In Ergänzung zu den Anträgen aus den Stellungnahmen der SBB und des Verbandes öffentlicher Verkehr beantragen wir daher:

1. im Kontext der VDSG im laufenden Gesetzgebungsverfahren zur Revision des PBG die Auswirkungen des neu gefassten Art. 54 PBG zu überprüfen und ggf. nötige Anpassungen oder

Präzisierungen so vorzunehmen, dass die Branche die Vorgaben umsetzen und auch den Interessen der Kundinnen und Kunden entsprochen werden kann.

2. die neuen Bestimmungen des Art. 54 PBG oder sich aus dem DSG beziehungsweise aus der VDSG ergebende Vorgaben dahingehend zu präzisieren,

    a. dass sich die Anwendung der datenschutzrechtlichen Vorschriften für Bundesorgane bei den konzessionierten Transportunternehmen – wenn überhaupt – auf die Grundpflichten des Transportvertrages und damit den Kauf bzw. die Ausstellung eines Fahrausweises sowie die eigentliche Beförderungsleistung begrenzt sowie

    b. dass sich in datenschutzrechtlicher Hinsicht bei der Erfassung und Bearbeitung von Verstössen gegen den Transportvertrag im Sinne von Art. 20 und 20a PBG für die Transportunternehmungen keine datenschutzrechtlichen Verpflichtungen ergeben, die über die entsprechenden Bestimmungen für private Personen hinausgehen.

In diesem Zusammenhang bitten wir um Klärung, ob sich unter Berücksichtigung der vorgesehenen Änderung des Art. 54 PBG, den Bestimmungen des DSG sowie den geplanten Regelungen in der VDSG nicht ein Widerspruch zu den Bestimmungen von Art. 20a PBG ergeben könnte, wonach Transportunternehmen bei Reisen ohne gültigen Fahrausweis in bestimmten Grenzen Daten austauschen können. Die bereits ausführlichen Regelungen gemäss Art. 20a PBG haben sich in den vergangenen Jahren auch mit Blick auf den Schutz von Daten bewährt. Sie helfen insbesondere Transportunternehmungen mit geringerem Aufkommen, bei Reisen ohne gültigen Fahrausweis vorsätzliche Handlungen von Reisenden von unbeabsichtigten Vorkommnissen zu unterscheiden. Dies vermeidet Entscheidungen sowie Datenhaltungen zu Ungunsten von Reisenden.

In allen übrigen Punkten schliessen wir uns wie erwähnt den Stellungnahmen des VöV und der SBB an. Wir bitten Sie um eine sorgfältige Abwägung sowie um eine praxisorientierte und rechtssichere Regelung für den berechtigten Schutz von Personendaten im öffentlichen Verkehr.

Abschliessend bitten wir Sie, die Thurbo AG im weiteren Erörterungsprozess in Anlehnung an den Vorschlag des VöV einzubeziehen.

Freundliche Grüsse
Thurbo AG

Claudia Bossert
Unternehmensleiterin

Patrick Frank
Geschäftsentwicklung & HR

Kopie an: Peter König (BAV), Elmar Suter (BAV), Ueli Stückelberger (VöV), Anselm Filliger (SBB RC)

veb.ch | Talacker 34 | 8001 Zürich
Telefon 043 336 50 30 | Fax 043 336 50 33 | info@veb.ch | www.veb.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik
Bundesrain 20
3003 Bern

Mailadresse: **jonas.amstutz@bj.admin.ch**

6. Oktober 2021

Stellungnahme zur Totalrevision VDSG

Sehr geehrte Damen, sehr geehrte Herren

Wir beziehen uns auf Ihre Publikation vom 23. Juni 2021 zur Vernehmlassung der Revision der Datenschutzverordnung. Gerne nehmen wir diese Möglichkeit wahr.

Der **veb.ch** vertritt als grösster Schweizer Verband für Rechnungslegung, Rechnungswesen und Controlling über 9 000 Mitglieder aus der gesamten Schweiz. Der veb.ch ist in der Berufsbildung gemäss Bundesgesetz über die Berufsbildung vom 13. Dezember 2002 die für das Finanz- und Rechnungswesen sowie Controlling zuständige Organisation der Arbeitswelt. Der Verband besteht seit 1936 und ist unter anderem Mitträger der Prüfungen der beiden eidgenössisch anerkannten Prüfungen in seinem Fachbereich. Expertinnen/Experten in Rechnungslegung und Controlling sowie Inhaberinnen/Inhaber des Fachausweises im Finanz- und Rechnungswesen sind heute in der schweizerischen Wirtschaft die anerkannten, hochqualifizierten Fachleute.

1. Allgemeines

Bei der Prüfung des E-VDSG haben wir den Eindruck gewonnen, dass die Überarbeitung der VDSG, zumindest teilweise, sowohl formell als auch inhaltlich unsorgfältig erfolgt ist. So enthält der Entwurf einerseits Bestimmungen, die keine Grundlage im Gesetz haben oder die sogar klar dem Willen des Gesetzgebers widersprechen.

Andererseits fehlen in manchen Bereichen eindeutige Regelungen, was insbesondere vor dem Hintergrund der strengeren und ausgeweiteten Strafbestimmungen im revidierten DSG problematisch ist. Unternehmen und Verantwortliche benötigen klare Vorgaben, um beispielsweise bei der Umsetzung von Datensicherheitsmassnahmen zukünftig eine Strafbarkeit zu vermeiden.

Im Folgenden gehen wir auf einige Bestimmungen genauer ein.

2. Datensicherheit

Art. 2 E-VDSG führt die Schutzziele der Datensicherheit auf, welche so bereits in der geltenden VDSG enthalten sind. Unserer Ansicht nach haben diese Schutzziele keine absolute Geltung und sind als veraltet zu bezeichnen. Zudem ist die Bestimmung zu detailliert formuliert.

Hingegen fehlen im E-VDSG klare Vorgaben über die Mindestanforderungen an die Datensicherheit, deren Regelung das Gesetz an den Verordnungsgeber delegiert hat. Das Fehlen entsprechender Bestimmungen ist insbesondere problematisch, da das revDSG die Verletzung der Mindestanforderungen an die Datensicherheit unter Strafe stellt. Eine detaillierte, praxistaugliche und unzweideutige Regelung dieses Punktes ist unserer Ansicht nach daher immanent wichtig.

3. Zusätzliche Dokumentationspflichten

Wir haben festgestellt, dass der E-VDSG eine Reihe von Dokumentationspflichten enthält, die im Gesetz nicht vorgesehen sind. Unserer Ansicht nach ist die Umsetzung dieser zusätzlichen Dokumentationspflichten für die Unternehmen mit einem hohen Aufwand verbunden. Insbesondere für KMU ist dieser zusätzliche Aufwand nicht tragbar. Hinzu kommt, dass durch diese zusätzlichen Dokumentationen kein Mehrwert für den Persönlichkeitsschutz geschaffen wird.

Für die in Art. 3 E-VDSG vorgesehene Protokollierungspflicht gibt es keine Grundlage im revDSG. Zudem ist die in Art. 3 Abs. 4 E-VDSG vorgesehene Regelung, nach der diese Protokolle während zwei Jahren getrennt vom Datenbearbeitungssystem aufbewahrt werden müssten, nur mit erheblichem Aufwand umsetzbar. Protokolle werden in und von jenen Systemen erzeugt, in denen die Daten bearbeitet werden. Um die Protokolle somit getrennt vom System aufbewahren zu könnten, müssten Unternehmen Kopien von allen anfallenden Protokollen auf externe Systeme übertragen. Die Erstellung der hierfür notwendigen Prozesse

und die Änderung von bestehenden Systemen wäre mit einem enormen, nicht vertretbaren Aufwand verbunden.

Auch die in Art. 4 E-VDSG vorgesehene Pflicht zur Erstellung eines Bearbeitungsreglements für Datenbearbeitungen mit einem hohen Risiko würde zu einem unnötigen Dokumentationsaufwand und zu einem erheblichen administrativen Aufwand führen. Unternehmen müssen die geforderten Angaben bereits bei der Durchführung von Datenschutz-Folgenabschätzung dokumentieren. Für uns ist daher nicht ersichtlich, inwiefern diese zusätzliche Dokumentation den Schutz der Persönlichkeit der betroffenen Personen erhöhen könnte. Zudem fehlt auch dieser Regelung gemäss unserer Einschätzung die gesetzliche Grundlage.

Auch die in Art. 16 sowie 19 Abs. 5 E-VDSG vorgesehenen Pflichten finden keine Grundlage im revDSG und können folglich nicht durch die Verordnung eingeführt werden.

4. Informationspflichten

Gemäss Art. 15 E-VDSG müssten die Unternehmen bei der Bekanntgabe von Personendaten die Empfänger neu über die Vollständigkeit der Daten informieren. Unseres Erachtens lässt sich diese Pflicht in der Praxis nicht sinnvoll umsetzen. Der Empfänger unterliegt ohnehin selber der Pflicht, sich zu vergewissern, dass die durch ihn bearbeiteten Daten richtig sind. Hinzu kommt, dass eine Grundlage im revDSG fehlt.

Wir sind daher der Ansicht, dass der Entwurf der Verordnung einer grundsätzlichen Überarbeitung bedarf.

Einige Bestimmungen des E-DSG, wie insbesondere die zusätzlichen Dokumentationspflichten, sind vor allem für KMU schlichtweg nicht umsetzbar, da mit einem unverhältnismässigen grossen Aufwand verbunden. Andererseits fehlen im E-DSG Punkte, deren Regelung das revDSG eigentlich an den Verordnungsgeber delegiert hat.

Wir bedanken uns im Voraus für die Berücksichtigung unserer Stellungnahme und stehen für allfällige Fragen gerne zur Verfügung.

Freundliche Grüsse

veb.ch

Herbert Mattle
Präsident

Prof. Dr. Dieter Pfaff
Vizepräsident

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz BJ
Bundesrain 20
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Bern, 4. Oktober 2021

Stellungnahme zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Damen und Herren

Am 23. Juni 2021 wurde die Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) eröffnet. Als nationaler Dachverband der Transportunternehmen des öffentlichen Verkehrs machen wir von der Möglichkeit zur Stellungnahme gerne Gebrauch.

Einleitend ist festzuhalten, dass gemäss den im Rahmen der hängigen RPV-Reform vorgesehenen Änderungen des Personenbeförderungsgesetzes (PBG) sich die Datenbearbeitung der konzessionierten Unternehmen künftig grundsätzlich nach den Bestimmungen für Bundesorgane richten soll. In diesem Zusammenhang gilt es zu erwähnen, dass der Personentransportvertrag von der Rechtsprechung und herrschenden Lehre nach wie vor als privatrechtlich qualifiziert wird. Die vorgesehene Änderung hat zur Folge, dass sämtliche konzessionierten Transportunternehmen im Bereich des Datenschutzes den Regelungen für Bundesorgane unterstehen, folglich kleine, mittlere und grosse Unternehmen. Die vorgesehenen Regelungen in der VDSG betreffend Bundesorgane würden jedoch Massnahmen erforderlich machen, welche für die Transportunternehmen sehr einschneidend wären und von ihnen kaum oder gar nicht umgesetzt werden könnten. Dies gilt umso mehr, da es sich beim öffentlichen Verkehr um ein Massengeschäft handelt**. Es ist offenkundig, dass ein konzessioniertes Transportunternehmen nicht mit einem hoheitlich handelnden Bundesorgan, welches der zentralen oder dezentralen Verwaltung angehört, gleichgesetzt werden kann**. Dieser Umstand muss soweit möglich in der VDSG berücksichtigt werden. Erforderlich sind Regelungen, die praxistauglich sind und mit angemessenen Mitteln umgesetzt werden können. Im Folgenden werden einzelne Punkte, die für den Verband öffentlicher Verkehr (VöV) und seine Mitglieder von zentraler Bedeutung sind, hervorgehoben. Im Übrigen wird auf die separat eingereichte ausführliche Stellungnahme der SBB, die Mitglied des VöV ist, verwiesen.

Dählhölzliweg 12
CH-3000 Bern 6
info@voev.ch
www.voev.ch

Für Bundesorgane besteht bei jeder automatisierten Bearbeitung von Personendaten eine Pflicht zur Protokollierung, unabhängig davon, ob ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht (vgl. Art. 3 Abs. 2 VDSG). **Diese Pflicht geht eindeutig zu weit und ist in der Praxis für die Transportunternehmen nicht umsetzbar.** Unter Berücksichtigung dieser Tatsache sowie dem Umstand, dass eine Verletzung der Protokollierungspflicht wohl als strafbare Verletzung der Datensicherheit zu qualifizieren wäre, erscheint diese Regelung als sehr problematisch. Im revidierten Datenschutzgesetz wurde zudem bewusst auf allgemeine Dokumentationspflichten verzichtet und an deren Stelle Regelungen zur Führung eines Bearbeitungsverzeichnisses vorgesehen. Es fehlt somit an einer gesetzlichen Grundlage. Dies gilt auch bezüglich der Bestimmungen zur Erstellung eines Bearbeitungsreglements (vgl. Art. 4 und 5 VDSG). **Diese Pflicht gilt bei Bundesorganen erneut unabhängig vom bestehenden Risiko. Sowohl die Pflicht zur Protokollierung wie auch zur Erstellung eines Bearbeitungsreglements sollte für Bundesorgane, wenn überhaupt – da eine gesetzliche Grundlage fehlt – nur bei einer umfangreichen Bearbeitung besonders schützenswerter Personendaten oder der Durchführung eines Profilings mit hohem Risiko bestehen.** Bezüglich den Tatbestandsvarianten des Zugänglichmachens von Personendaten und der Verknüpfung von Datenbeständen gemäss Art. 5 Abs. 1 Bst. d und e VDSG ist ausserdem unklar, was konkret damit gemeint ist.

Gemäss Art. 27 VDSG muss jedes Bundesorgan eine Datenschutzberaterin oder einen Datenschutzberater ernennen. Mehrere Bundesorgane können gemeinsam jemanden bestimmen. Auch diese Regelung geht zu weit und ist in der Praxis mit verhältnismässigen Mitteln nicht umsetzbar. Für die Pflicht der Ernennung einer Datenschutzberaterin oder eines Datenschutzberaters fehlt es überdies erneut an einer gesetzlichen Grundlage. Es sollte an der bisherigen Regelung für Bundesorgane festgehalten werden, folglich, dass es dem Bundesorgan freisteht, eine Datenschutzberaterin oder einen Datenschutzberater zu ernennen. Es wäre im Übrigen fraglich, wie namentlich kleine Transportunternehmen dieser Pflicht gerecht werden könnten, wobei sie auch für grössere Unternehmen belastend wäre, hier im Wesentlichen aufgrund der ausserordentlich hohen Anzahl vorgenommener Datenbearbeitungen. Die Einsetzung einer gemeinsamen Datenschutzberaterin oder eines gemeinsamen Datenschutzberaters für mehrere Transportunternehmen oder sogar für die ganze Branche wäre ebenfalls kaum realisierbar, da die betreffende Person u.a. mit den Abläufen des jeweiligen Unternehmens vertraut sein muss, um ihre Aufgaben fachgerecht ausführen zu können.

Art. 7 VDSG hält sodann fest, dass das Bundesorgan die Datenschutzberaterin oder den Datenschutzberater über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten informiert. Diese Informationspflicht gilt auch bei Problemen bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften. **Für die Transportunternehmen ist diese Regelung zu umfassend und nicht praktikabel, insbesondere greift sie in die interne Organisationsfreiheit ein.** Die Bestimmung lässt überdies einen grossen Interpretationsspielraum zu, da nicht klar ist, was unter den Begriff «Probleme» fällt, sprich, wann genau die Datenschutzberaterin oder der Datenschutzberater benachrichtigt werden müsste. **Aufgrund des Art. 10 Abs. 2 Bst. b revDSG, der ausdrücklich vorsieht, dass die Datenschutzberaterin oder der Datenschutzberater bei der Anwendung der Datenschutzvorschriften mitwirkt, erscheint Art. 7 VDSG zudem überflüssig.**

Hinsichtlich der Informationspflichten gemäss Art. 15 und 16 VDSG ist festzuhalten, dass sich diesbezüglich keine Grundlage im revidierten Datenschutzgesetz finden lässt. Es ist deshalb fraglich, ob diese Pflichten auf Verordnungsstufe geregelt werden können. Die Umsetzung wäre darüber hinaus sehr einschneidend bzw. kaum möglich. Die Regelungen erscheinen ausserdem überflüssig, da der Verantwortliche sicherzustellen hat, dass die Datenschutzgrundsätze eingehalten werden. Dies wird in der öV-Branche für den Bereich des direkten Verkehrs (vgl. Art. 16

Personenbeförderungsgesetz[1]) mittels einer Branchenregelung – dem Übereinkommen der Alliance SwissPass (Nationale Organisation zur Zusammenarbeit der am Direkten Personenverkehr Teilnehmenden), kurz Ue500 – welche vom Bundesamt für Verkehr genehmigt worden ist, gewährleistet.

Gestützt auf obgenannte Ausführungen vertritt der VöV die Haltung, dass die neuen Regelungen für Bundesorgane, welche bei den konzessionierten Transportunternehmen zur Anwendung gelangen, für letztere zu einschneidend und mit den vorhandenen Ressourcen kaum oder gar nicht umsetzbar wären, was sehr problematisch ist. Dies gilt auch bezüglich des Umstandes, dass es bei vielen Bestimmungen an einer gesetzlichen Grundlage fehlt.

Es sollten Regelungen vorgesehen werden, die mit dem revidierten Datenschutzgesetz im Einklang stehen und sowohl für Bundesorgane der zentralen sowie dezentralen Verwaltung als auch für die konzessionierten Transportunternehmen in der Praxis mit verhältnismässigem Aufwand durchführbar sind.

Da die Thematik der Datenbearbeitung im öffentlichen Verkehr sowohl inhaltlich wie auch von den betroffenen «Playern» her sehr komplex ist, würden wir es sehr begrüssen, wenn das BJ diesbezüglich die involvierten Stellen (BAV, EDÖB, SBB, VöV, ASP, PAG u.a.) **zu einer Besprechung/einem Runden Tisch** einladen würde, damit für die offenen Punkte eine möglichst allseits befriedigende Lösung gefunden werden kann.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und würden uns – wie oben erwähnt – sehr freuen, Sie würden eine solche Besprechung einberufen.

Freundliche Grüsse

Ueli Stückelberger
Direktor VöV

[1] Im Fern-, Regional- und Ortsverkehr bieten die Unternehmen in der Regel der Kundschaft für Verbindungen, die über das Netz verschiedener Unternehmen führen, einen einzigen Transportvertrag an. Soweit ein Bedürfnis besteht, ist im Fern- und Regionalverkehr zwingend ein direkter Verkehr anzubieten. Sie erstellen dafür gemeinsame Tarife und Fahrausweise.

Entwurf E-VDSG | Stellungnahme

14. Oktober 2021

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrter Herr Amstutz,
Sehr geehrte Damen und Herren

Wir danken Ihnen für die uns angebotene Gelegenheit, zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) Stellung nehmen zu dürfen. Nachfolgend erhalten Sie fristgerecht unsere Überlegungen zu dieser bedeutenden Umsetzungsnorm im Bereich des Datenschutzes. Dabei nehmen wir vorweg, dass sich unsere Stellungnahme auf den eigentlichen Text des E-VDSG fokussiert und nicht auf alle noch zusätzlichen Verordnungsänderungen (Anhang 2 des Entwurfs). Zudem konzentrieren wir uns, aufgrund unserer Tätigkeit, insbesondere auf den privatrechtlichen Teil der Regelung. Dies bedeutet nicht, dass der öffentlich-rechtliche Teil in allen Punkten unproblematisch erscheint.

1. Allgemeine Vorbemerkung

1.1. VSI als Dienstleister im Interesse der Wirtschaft

Seit 1941 widmet sich der Verband Schweizerischer Inkassotreuhandinstitute (VSI) in der Form eines Vereins der Aufgabe, das Inkassowesen und verwandte Rechtsgebiete in der Schweiz zu fördern und strebt die Verbesserung der gesetzlichen Grundlagen und die Bekämpfung von Missbräuchen an. Die Verbandsmitglieder helfen mit, die schweizerische Volkswirtschaft vor Zahlungsausfällen zu schützen und setzen sich darüber hinaus für die Interessen der Gläubiger ein. Weiter setzt sich der VSI für ein unternehmensfreundliches Umfeld und optimale wirtschaftliche Rahmenbedingungen für die Mitglieder ein. Die im VSI organisierten Unternehmen sind für das Inkasso von über 10 Milliarden Schweizer Franken zuständig. Jährlich kassieren die Inkassounternehmen rund 700 Millionen Franken ein.

1.2. Stellung des Vereins im Rahmen des Datenschutzrechts

Durch unsere Tätigkeit bearbeiten wir Personendaten von betroffenen Personen, in der Regel mögliche künftige Vertragspartner unserer Mitglieder. Dabei ist es wichtig einen Fehler auszuräumen, welcher von Zeit zu Zeit in der Lehre begangen wird. Verschiedentlich werden durch das neue Datenschutzrecht Anforderungen an den Verantwortlichen gestellt, wenn er umfangreich besonders schützenswerte Personendaten bzw. wenn er ein Profiling mit hohem Risiko durchführt. Wirtschaftsauskünfte sind weder von der einen noch von der anderen Tätigkeit betroffen (siehe stellvertretend für andere Beispiele Art. 4 Abs. 1 E-VDSG):

- Zum einen verarbeitet unser Verband keine besonders schützenswerte Personendaten. Im Gegenteil: Sie bezieht eine Vielzahl ihrer Informationen von öffentlich zugänglichen Registern.

- Zum anderen wird durch die Auskunft über die Bonität eines möglichen Kunden kein Profiling mit hohem Risiko für die Persönlichkeitsrechte der betroffenen Person durchgeführt. Dies aus mehreren Gründen:

    - Erstens ist das hauptsächliche Risiko, welches von der betroffenen Person eingegangen wird, die Zahlungsart für die Lieferung eines Gutes oder die Erbringung einer Dienstleistung. Es geht lediglich darum, die Kreditwürdigkeit einer Person abzuschätzen. Dabei verliert die betroffene Person weder ein Recht noch einen Anspruch, falls die Prüfung ein negatives Bild aufzeigt. Es gibt nämlich weder ein Anrecht noch einen Anspruch auf die Erbringung von Dienstleistungen gegen Kredit. Die betroffene Person kann die Vertragsleistung ohne Weiteres gegen Vorkasse, Barzahlung oder Sicherheiten beziehen, was auch in der Regel die Bezahlungsart bei den meisten Verträgen im täglichen Umgang ist.

    - Im Gegenteil: Die Überprüfung der Kreditwürdigkeit dient sowohl dem Gläubiger als auch dem Schuldner. Dies zeigt bereits das Bundesgesetz über den Konsumkredit vom 23. März 2001 (SR 221.214.1), welches in Art. 22 ausdrücklich die Kreditfähigkeitsprüfung zum Zweck der Vermeidung einer Überschuldung der Konsumentin oder des Konsumenten infolge eines Konsumkreditvertrags vorsieht. Nichts anderes bezweckt die Tätigkeit unseres Verbandes. Es ist weder im Sinne des Gläubigers noch im Sinne des Schuldners oder der Gesamtwirtschaft, dass die Überschuldung der Konsumenten zu einem Vertrauensverlust führt.

- Die Berechtigung, für den künftigen Gläubiger, seine Leistungen nur bei einer positiven Risikobewertung gegen Kredit zu erbringen, hängt auch sehr stark mit der Ineffizienz der Betreibungs- und Konkursverfahren zusammen. In aller Kürze: Eine statistische Aufarbeitung hat uns gezeigt, dass nur rund 2% der Konkurseröffnungen abgeschlossen werden können. 98% werden aufgrund der Kosten gar nicht beendet. Die beendeten Konkursfälle führen zu einer Konkursdividende der Gläubiger von rund 5% der eingegebenen Forderungen. Der Staat ist gegenwärtig nicht in der Lage, einem Gläubiger ein erfolgsversprechendes Konkursverfahren anzubieten, weshalb es unerlässlich ist, das Gläubigerrisiko entsprechend anders minimieren zu können.

2. Vorbemerkung zum E-VDSG

2.1. Das VDSG als Ausführungsgesetzgebung zum DSG

In rechtsstaatlicher Hinsicht bedarf der Inhalt einer Verordnung einer genügenden Abstützung im Gesetz. Insbesondere muss die Delegationsnorm die vom Bundesrat vorgeschlagene Regelung rechtfertigen. Nicht zulässig ist, in einer Verordnung Regelungen nachzuschieben, welche das Parlament abgelehnt hat oder Nachbesserungen nachzureichen, welche im Gesetzgebungsverfahren überhaupt nicht berücksichtigt wurden.

Nicht alle vorgeschlagenen Lösungen im E-VDSG genügen dieser rechtsstaatlichen Anforderung. Im Gegenteil: **Der Entwurf enthält Regeln, die entweder ausdrücklich vom Parlament abgelehnt worden sind, die zumindest in systematischer Hinsicht vom Parlament anders gewählt wurden oder an die der Gesetzgeber in keiner Weise gedacht hat. Diese Vorschläge sind allesamt aus dem E-VDSG zu löschen.** Wir verweisen dabei auf die Bemerkungen zu den einzelnen Bestimmungen.

2.2. Das VDSG als Instrument zur Erreichung der Euro-Kompatibilität

Wie beim DSG hat der Bundesrat auch beim E-VDSG in seinen Erläuterungen festgehalten, dass es lediglich um die Angemessenheit des Schweizerischen Datenschutzrechts im Vergleich zur europäischen DSGVO geht. In keiner Art und Weise wurde je von einer Erweiterung der Einschränkungen bei den Datenbearbeitungen bzw. von einer strengeren Regelung gesprochen. Diesem Ziel bleibt also der Bundesrat auch bei der Formulierung des VDSG ausdrücklich verpflichtet. **Alle Bestimmungen, welche also über die Erfordernisse des E-VDSG hinausgehen müssen als zweckfremd und als unzulässig abgelehnt werden. Auch diese sind aus dem E-VDSG zu löschen.**

2.3. Formelle Bemerkung

Zur besseren Lesbarkeit der Verordnung und zum klareren Bezug zum DSG würden wir klare Verweise auf die betroffenen Gesetzesbestimmungen im Titel der jeweiligen Bestimmungen begrüssen. Mit dieser Gesetzgebungstechnik muss sich der Bundesrat klarer und eindeutiger zur Delegationsnorm beziehen, was im vorliegenden Entwurf nur suboptimal gelingt.

3. Zu den einzelnen Bestimmungen

Art. 1 Abs. 1 Bst. d

Als Art. 1 Bst. d werden als Kriterium der Angemessenheit für die Datensicherheit die «Implementierungskosten» genannt. Es wird begrüsst, dass der Aufwand für die Verantwortlichen auch ausdrücklich in die Angemessenheitsüberprüfung aufgenommen wird. Der verwendete Begriff erscheint jedoch problematisch, da er lediglich auf die geldwerten Umsetzungsaufwendungen beschränkt werden könnte (siehe auch S. 16 der Erläuterungen). Für eine solche Einschränkung gibt es keinen Grund. Statt den Begriff «Implementierungskosten» schlagen wir vor den allgemeineren Begriff «**Aufwand für den Verantwortlichen**» zu verwenden. Es gibt keinen Grund, beim Verantwortlichen überhöhte Planungs- oder Projektkosten auszulösen, nur um festzustellen, ob die Implementierung dann ihrerseits verhältnismässig ist.

Art. 1 Abs. 2

Diese Bestimmung verlangt die Überprüfung der technischen und organisatorischen Massnahmen in angemessenen Abständen (gemeint sind hier die zeitlichen Abstände…). Aufgrund des risikobasierten Ansatzes der gesamten Thematik der Datensicherheit erscheint diese Regelung falsch. Zudem führt die Herleitung der Formulierung vom Abs. 1 zur sprachlich merkwürdigen Aussage, dass die dem Risiko angemessenen Massnahmen in angemessenen Abständen zu überprüfen sind. Der Begriff der Angemessenheit riskiert zum Gummibegriff zu verkommen, der jedes Mal verwendet wird, wenn man nichts Präzises auszusagen weiss. Zudem ist fraglich, ob mit der vom Bundesrat aufgestellten Forderung der Überprüfung in angemessenen Abständen die Delegationsnorm von Art. 8 Abs. 3 revDSG eingehalten wird. Die Mindestanforderungen an die Datensicherheit rechtfertigen keine Einführung zusätzlicher Kriterien, welche im Gesetz nicht verankert sind. Es ist – wenn überhaupt – in materieller Hinsicht zu fordern, dass ein Zusammenhang zwischen der Überprüfung der Datensicherheit und der Entwicklung des Risikos hergestellt wird. Vorschlag: «**Die Massnahmen sind bei einer relevanten Veränderung des Risikos zu überprüfen**.»

Art. 2, Einleitungssatz

Die Bestimmung spricht von Zielerreichung. Die jeweiligen Pannen der Swisscom zeigen mit aller Deutlichkeit das auf, was man seit jeher weiss: Die absolute Datensicherheit gibt es nicht. Von den Verantwortlichen zu verlangen, dass die entsprechenden Schutzziele erreicht werden, ist weder korrekt noch realistisch. Der Bereich der Datensicherheit ist ein typischer Bereich, bei welchem keine Ergebnisverantwortung, sondern nur eine Sorgfaltspflicht auferlegt werden darf. Deshalb ist die Bestimmung wie folgt umzuformulieren: «Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele anstreben:» Nur so dürfen in der nachfolgenden Aufzählung Begriffe wie «verwehrt», «verunmöglicht», «verhindert», «gewährleistet», usw. überhaupt verwendet werden. Ansonsten müssen in der Aufzählung die Schutzziele jeweils vernünftig relativiert werden, was sicher nicht zur Klarheit der Formulierung beiträgt.

Art. 2, Bst. a bis k:

Art. 2 dürfte eigentlich nur Schutzziele nennen, welche vom Verantwortlichen angestrebt werden können. Gerade die Transportkontrolle kann beispielsweise durch viele externe Faktoren gefährdet werden, für welche der Verantwortliche nicht einstehen kann. Die Aufzählung von Art. 2 Bst. a bis k zeigt in aller Deutlichkeit, was in der Lehre verschiedentlich moniert worden ist: Mangels Effizienz der staatlichen Interventionen, wird die Last der «Privacy by design» vollumfänglich auf den Verantwortlichen abgewälzt, statt dass sie zu datenschutzfreundlichen Technologien durch die Hersteller von Hard- und Software führen würde. Diese Entwicklung zulasten der Nutzer von Informationstechnologien ist im höchsten Masse problematisch, da damit auch der Aufwand für die Datensicherheit dem Betreiber und nicht dem Entwickler von Informationstechnologien auferlegt wird. Die Aufzählung in Art. 2 Bst. a bis k ist in Beachtung dieser Problematik zu überarbeiten und dem Verantwortlichen dürfen nur Schutzziele auferlegt werden, die auch tatsächlich in seiner Verantwortung
liegen.

Art. 3

Der Begriff der Protokollierung wird im DSG nirgends verwendet, im Gegenteil z.B. zum neuen Art. 78 Abs. 5 Nachrichtendienstgesetz vom 25. September 2015 (NDG - SR 121) bzw. zum neuen Art. 10 Abs. 3 Finanzkontrollgesetz vom 28. Juni 1967 (FKG - SR 614.0). Die nun in der Verordnung vorgesehenen Anforderungen an die Protokollierung übersteigen jedes vernünftige Mass und führen zu einer Bürokratie, welche in keinem

Verhältnis zum tatsächlichen Nutzen der Anforderungen steht. Insbesondere die Aufbewahrungsdauer der Protokolle von 2 Jahren (Art. 3 Abs. 4 E-VDSG) ist absolut unangemessen.

Die Protokollierung ist eine qualifizierte Dokumentation der Datenbearbeitung von Personendaten, sagt sie doch ganz klar etwas darüber aus, wer, wann, wie und in welchem Masse Daten der betroffenen Person verarbeitet hat (Art. 3 Abs. 3 E-VDSG). Eine Protokollierung schafft somit ein Spannungsfeld zwischen dem Schutz der betroffenen Person und dem Schutz der verarbeitenden Person. Das Profiling führt zu einer qualifizierten und automatisierten Bearbeitung der Personendaten der datenbearbeitenden Person. Sie bedarf demnach auch einer Rechtsgrundlage im formellen Gesetz, insbesondere dann, wenn die Bearbeitung dieser Personendaten im beruflichen Umfeld zu einem eigentlichen Profiling (Art. 5 Bst. f revDSG) und zu einer verpönten Verhaltenskontrolle des Arbeitnehmenden verkommen sollte.

Die nachträgliche Einführung der Protokollierungspflicht im Rahmen der Verordnung erscheint aus Sicht der Wirtschaft nichts anderes als eine unrechtmässige bundesrätliche Nachbesserung eines im Parlament erfolgten Kompromisses, welches zum Verzicht der Protokollierungspflicht geführt hat. Aus Sicht der Wirtschaft genügt die Pflicht der Erstellung die Pflicht zur Erstellung eines Verzeichnisses der Datenbearbeitungen vollumfänglich, um die Rechte und die Interessen der betroffenen Personen zu wahren.

Art. 4

Die Anforderungen von Art. 4 E-VDSG gehen auch viel zu weit. Selbst mit der Einschränkung von Art. 4 Abs. 1 E-VDSG wäre beispielsweise nicht zu verhindern, dass viele Einpersonenunternehmen (Rechtsanwälte, Treuhänder usw.) ein solches Bearbeitungsreglement verfassen müssten. Falls man also diese Pflicht beibehalten muss, ist deren Anwendungsbereich nochmals sorgfältig zu umschreiben
und einzugrenzen (schon fast grotesk mutet bei Einpersonenunternehmen nämlich Art. 4 Abs. 3 E-VDSG an).

Allgemein stellt sich die Frage, welchen Mehrwert sich der Bundesrat aus der Führung eines Bearbeitungsreglements neben der Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungen
erhofft.

Sollte widererwarten am Bearbeitungsreglement festgehalten werden, dann führt die Pflicht, das Bearbeitungsreglement «regelmässig» zu aktualisieren (Art. 4 Abs. 3 E-VDSG) nur dazu, dass eine grosse Mehrheit der Datenbearbeiter dieser Kategorie mit bürokratischen Mitteln in die Illegalität gedrängt werden. Es gibt überhaupt keinen nachvollziehbaren Grund zur «regelmässigen» Überarbeitung des Bearbeitungsreglements. Dieses muss dann überarbeitet werden, wenn es einen Anlass zur Aktualisierung gibt (Veränderung der Bearbeitungsmittel oder Formen).

Art. 5

Obwohl Art. 5 E-VDSG lediglich Bundesorgane betrifft, sei hier dennoch erwähnt, dass eine übertriebene Bürokratie in diesem Bereich zur unnötigen Verschwendung von Ressourcen und Steuergeldern führt, die anderswo wohl effizienter und nützlichere insbesondere für die Empfänger eingesetzt werden können. Wir verzichten auf die erneute Erwähnung dieser Bemerkung in den folgenden Bestimmungen, welche den Ressourceneinsatz der Bundesorgane beeinflussen. Die Bemerkung gilt aber selbstverständlich allgemein.

Art. 6, Abs. 1 und 2

Die Pflicht, für den Verantwortlichen, die vertrags- und gesetzesmässige Bearbeitung durch den Auftragsbearbeiter «sicherzustellen» ist konzeptionell schlicht falsch. Richtig ist, dass der Verantwortliche sich gemäss Art. 9 Abs. 2 DSG vergewissern muss, dass die Datenbearbeitung korrekt erfolgt (korrekt in Art. 6 Abs. 2, 1. Satz E-VDSG). Diese unverhältnismässige, nicht einzuhaltende und nicht vom Gesetzgeber vorgesehene Verschärfung der Pflicht des Verantwortlichen ist im Rahmen der Delegation an den Bundesrat als unrechtmässig zu betrachten. Die Vergewisserung ist ein Streben nach Rechtmässigkeit und eine Kontrollpflicht im Rahmen des Auftrages.

Formulierungsvorschläge für Art. 6 Abs. 1, 2. Satz bzw. Art. 6 Abs. 2, 2. Satz E-VDSG:

Er vergewissert sich, dass die Daten vertrags- und gesetzesgemäss bearbeitet werden.

Andernfalls muss er sich auf dem vertraglichen Weg vergewissern, dass ein gleichwertiger Datenschutz gewährleistet wird.

Art. 6, Abs. 3

Verschiedentlich wird im Gesetz eine «schriftliche» Form verlangt. Es wäre wohl an der Zeit, dass sich der Gesetzgeber ein für alle Mal dieser Thematik annimmt und entscheidet, ob die «Schriftform» noch zeitgemäss ist, oder ob nicht systematisch die modernere Fassung «in einer Form, die den Nachweis durch Text ermöglicht» ersetzen sollte. Natürlich ist der E-VDSG vielleicht nicht gerad die optimale Revision für einen solchen Systementscheid. Es schadet jedoch nichts, dass eine solche Verordnung zukunftskompatibel formuliert wird. Wir verzichten auf die Erwähnung dieser Bemerkung in anderen Bestimmungen, welche die Schriftlichkeit erfordern.

Art. 8

Lediglich im erläuternden Bericht wird klargestellt, an wer sich diese Bestimmung richtet und wen eine Handlungspflicht trifft. Da diese selbstverständlich nicht den privaten Datenbearbeiter betreffen kann, ist dies unmissverständlich im Verordnungstext festzuhalten. Z.B. im Einleitungssatz von Art. 8 Abs. 1 (Änderung in fetter Schrift hervorgehoben): «… einen angemessenen Schutz gewährleistet, **hat der Bundesrat namentlich folgende Kriterien zu berücksichtigen**…».

Art. 9, Abs. 1

Unklar ist, nach welcher Gesetzgebung die Einhaltung der Voraussetzungen gemäss der Aufzählung von Art. 9 Abs. 1 Bst. a – k E-VDSG zu erfüllen sind. Die Kriterien dürfen nicht kumulativ alle möglichen Rechtssystemen unterstellt werden, sonst kann das der Verantwortliche nicht mehr handhaben.

Art. 9, Abs. 2

Auch hier ist die Forderung an den Verantwortlichen überrissen, wenn er «sicherstellen» muss. Auch hier muss er sich «vergewissern».

Art. 10, Abs. 1

Auch hier ist die Forderung an den Verantwortlichen überrissen, wenn er «sicherstellen» muss. Auch hier muss er sich «vergewissern».

Art. 12 Abs. 2 und 3

Es ist unklar, ob die aus Art. 12 Abs. 2 und 3 E-VDSG abgeleiteten Voraussetzungen den Anwendungsbereich von Kodizes und Zertifizierungen nicht unangemessen einschränken. Vielmehr scheint es erforderlich auf die Gesamtwirkung dieser Instrumente zu achten und diese allenfalls vom EDÖB absegnen zu lassen (siehe auch Art. 44 E-VDSG). So könnte z.B. ein Absatz 4 folgendes Ergänzen:

4 Die vorstehenden Absätze 2 und 3 sind nicht anwendbar, wenn der EDÖB den Verhaltenskodex oder die Zertifizierung genehmigt hat.

Art. 13 Abs. 1

Gemäss Art. 19 Abs. 1 revDSG liegt die Informationspflicht klar beim Verantwortlichen und nicht beim Auftragsbearbeiter. Es kann zwar allenfalls eine vertragliche Delegation der Pflichterfüllung stattfinden, aber grundsätzlich ist es systemwidrig beide gleichzeitig in die Pflicht zu nehmen. Man könnte höchstens das «und» mit einem «oder» ersetzen.

Art. 15 und 16

Diese Bestimmungen findet keine Stütze im DSG und sind ersatzlos zu streichen. Die Berichtigung, Löschung, Vernichtung oder Einschränkung der Bearbeitung von Personendaten (Art. 16 E-VDSG) erfolgen zudem im Interesse der betroffenen Person. Diese müssen ja so oder so den Anforderungen des Gesetzes entsprechen. Wieso ausgerechnet in solchen Situationen eine neue Informationspflicht im Interesse der betroffenen Person liegen soll, ist nicht klar. Im Gegenteil: Mit einer solchen Information, sei sie auch noch so klar, wird die betroffene Person oft verunsichert oder zumindest auf einen Umstand aufmerksam gemacht, der dazu führt, dass Fragen aufgeworfen werden und Aufwand generiert wird, der dem Verantwortlichen nicht entschädigt wird. Das wird von der Wirtschaft in nachvollziehbarer Weise als unnötige und bürokratische Schikane empfunden. Mit

einer solchen neuen Pflicht fördert der Bundesrat nicht den Datenschutz, sondern den Datenschmutz. Auf unnötige Informationen ist in den Beziehungen zwischen dem Datenbearbeiter und der betroffenen Person zu verzichten.

Art. 18

Zum Kriterium der Schriftlichkeit, siehe die vorstehende Bemerkung zu Art. 6 Abs. 3 E-VDSG.

Die Aufbewahrungsfrist von **2 Jahren nach Beendigung der Datenbearbeitung** entbehrt einer gesetzlichen Grundlage im DSG und ist als zu lange zu betrachten. Die Aufbewahrung hat höchstens bis zur Beendigung der entsprechenden Datenbearbeitung zu dauern, da danach keine Verletzung der Rechte der betroffenen Person mehr erfolgen kann. Für die Frage, ob jemand durch die Datenbearbeitung ein Schutzrecht der betroffenen Person verletzt hat, ist nicht die Datenschutz-Folgenabschätzung relevant, sondern die konkrete Datenbearbeitung und die entsprechenden Verzeichnisse und Reglemente des Verantwortlichen.

Art. 19, Erläuterung

In den Erläuterungen des Bundesrates zeigt der Verfasser in den Bemerkungen zu Art. 19, dass er ein merkwürdiges Verständnis der deutschen Sprache hat. «Voraussichtlich» heisst überhaupt nicht, dass die Meldung in jedem «Zweifelsfall», in welchem ein «hohes Risiko nicht ausgeschlossen werden kann» zu erfolgen hat. Hat die Meldung bei einer «voraussichtlichen Verletzung zu erfolgen, dann ist diese nur vorzunehmen, wenn die Gefahr, dass eine Verletzung der Rechte der Betroffenen Person erfolgt ist, als klar höher einzustufen sind als die Chancen, dass keine Verletzung erfolgt ist. Der Bundesrat versucht in unrechtmässiger Art und Weise die Einschränkung des Gesetzgebers durch seinen Kommentar umzubiegen.

Art. 19 Abs. 1 Bst. b bis d

Diese Kriterien sind dem Gesetz nicht zu entnehmen. Der Bundesrat hat weder eine Delegation noch eine Ermächtigung erhalten, revArt. 24 DSG zu ergänzen. Deshalb sind diese Buchstaben aus der Verordnung zu streichen.

Art. 19 Abs. 1 Bst. e

Bei der Entdeckung einer Verletzung der Datensicherheit ist es eben gerade nicht immer möglich, die Folgen und die allfälligen Risiken umgehend und abschliessend festzustellen. Deshalb muss beim Bst. e «soweit möglich» vorangestellt werden.

Art. 19 Abs. 3

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 Abs. 4 revDSG hinausgeht.

Art. 19 Abs. 5

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 revDSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wider Erwarten an einer Dokumentationspflicht festhalten, schiessen die 3 Jahre weit über das Ziel hinaus. Eine Aufbewahrungsdauer kann höchstens ein Jahr betragen.

Art. 20 Abs. 1 und 2

Zum Kriterium der Schriftlichkeit, siehe die vorstehende Bemerkung zu Art. 6 Abs. 3 E-VDSG.

Art. 20 Abs. 5

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 25 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wiedererwarten an einer Dokumentationspflicht festhalten, schiessen die 3 Jahre weit über das Ziel hinaus. Eine Aufbewahrungsdauer kann höchstens ein Jahr betragen.

Art. 22

Der Fristenlauf kann selbstverständlich nur dann beginnen, wenn das Auskunftsgesuch formell korrekt eingereicht und inhaltlich klar ist. Solange das Gesuch entweder formell oder inhaltlich unklar ist, kann die Frist nicht laufen. Dies muss im Art. 22 E-VDSG in aller Klarheit zum Ausdruck kommen.

Art. 23

Aufgrund der Einschränkungen, die gemäss Abs. 1 für die Kostenbeteiligung vom Bundesrat aufgestellt werden, ist der unveränderte Betrag von CHF 300 geradezu lächerlich. Bei Aufwendungen, die CHF 1'000 weit übersteigen können, ist eine Kostenbeteiligung von nur gerade CHF 300.- nicht angemessen. Natürlich hat der Verantwortliche die Kosten zu belegen. Aber es kann nicht sein, dass der Verantwortliche auf einem Kostenberg sitzenbleibt und vom Kostenverursacher nur ein quasi symbolischer Betrag verlangt werden kann. Der Höchstbetrag ist deshalb anzuheben und sollte auf mindestens CHF 1'000 festgelegt werden.

Art. 24

Der Anspruch auf Datenportabilität bei der Datenherausgabe oder -übertragung darf nicht ein absoluter sein. Dieser Anspruch darf nur bestehen, soweit die Bearbeitung von Personendaten in gängigen Formaten erfolgen kann bzw. erfolgt.

Art. 45 Abs. 1 und 2

Wenn die Kostenbeteiligung nach Art. 23 mit den Gebührengrundsätzen des EDÖB verglichen werden, dann muss von einer krassen Diskrepanz gesprochen werden. Der EDÖB erledigt eine Tätigkeit im Interesse der Gesellschaft und es gibt keinen nachvollziehbaren Grund, weshalb die Person, welche Dienstleistungen von ihm braucht, um sich datenschutzkonform zu verhalten, derart abgeschröpft wird. Weder kann es sein, dass die Gebühren nach Zeitaufwand berechnet werden (die Privatperson hat keinen Einfluss auf die Effizienz der Leistungserbringung durch den EDÖB), noch sind die Stundensätze von CHF 150 bis 350 in irgendeiner Weise angemessen. Diese Gebührenbestimmung stiftet die hilfesuchende Privatperson geradezu an, das Datenschutzrecht zu verletzen da sie sich die Unterstützung durch den EDÖB nicht leisten kann. Die Gebührenordnung ist vollständig zu überdenken und nach einem vernünftigen Mass anzupassen. Es kann nicht sein, dass der Gesetzgeber einerseits für die Einhaltung des Datenschutzrechts einsteht und andererseits sich durch die Dienstleistungen des EDÖB bereichern will. Hier wird dem service-public-Gedanken in gröbster Art und Weise entgegengewirkt. Es ist erforderlich, Maximalgebühren für Tätigkeiten festzulegen, welche der Einhaltung des Datenschutzrechts dienen (z.B. Art. 59 Abs. 1 Bst. c revDSG, Konsultation aufgrund einer Datenschutz-Folgenabschätzung).

Sehr geehrter Herr Amstutz, wir bitten Sie um Kenntnisnahme und um Übernahme der vorstehenden Vorschläge, damit die VDSG in ihrer Rechtssicherheit und in ihrer Rechtmässigkeit entsprechend gestärkt werden kann.

Freundliche Grüsse

Patrik Odermatt

Daniel Bucklar

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Frau Bundesrätin Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Per Mail zugestellt an: jonas.amstutz@bj.admin.ch

Datum 13. Oktober 2021
Kontaktperson Thomas Rauch
Direktwahl 061 206 66 22
E-Mail t.rauch@vskb.ch

Stellungnahme der Kantonalbanken zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz

Sehr geehrte Frau Bundesrätin,
sehr geehrter Herr Amstutz,
sehr geehrte Damen und Herren

Am 23. Juni 2021 hat das Eidgenössische Justiz- und Polizeidepartement (EJPD) die Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) eröffnet. Wir danken Ihnen für die Gelegenheit zur Stellungnahme zu dieser wichtigen Vorlage.

Die vom Verband Schweizerischer Kantonalbanken vertretenen Kantonalbanken sind ebenfalls Mitglieder der Schweizerischen Bankiervereinigung. Die **Stellungnahme der Bankiervereinigung (SBVg)** wurde von den Kantonalbanken wesentlich mitgeprägt. Sie wird deshalb vollumfänglich unterstützt, weshalb **darauf verwiesen wird**.

Die Kantonalbanken heben nachfolgend die für sie wichtigsten Punkte hervor.

Wichtigste Anliegen der Kantonalbanken

1. **VDSG prinzipien- und risikobasiert ausgestalten**
   Zweck der VDSG ist es, die Bestimmungen des Bundesgesetzes über den Datenschutz (DSG) näher auszuführen. Der Entwurf zur VDSG enthält jedoch Regelungen, welche über eine blosse Konkretisierung des revidierten Datenschutzgesetzes hinausgehen. Während das neue Datenschutzgesetz prinzipien- und risikobasiert ausgestaltet ist, sind zahlreiche Regelungen des Verordnungsentwurfs unnötig detailliert und regelbasiert (vgl. die zahlreichen Anforderungskataloge). Dies verunmöglicht die Anwendung eines vernünftigen Ermessens durch den Datenbearbeiter, namentlich entsprechend dessen Grösse, Struktur, Komplexität, Risiken und Geschäftsmodell. Teilweise gehen die Regelungen sogar über das Niveau der Europäischen Datenschutzgrundverordnung (EU-DSGVO) hinaus und schaffen dadurch unnötige, die EU-Äquivalenz gefährdende und kontraproduktive «Swiss Finishes». Dies ist nicht angezeigt. Die Verordnung sollte den Geist des Gesetzes aufnehmen und dessen Regelungen prinzipien- und risikobasiert weiter ausführen und auch nicht darüber hinausgehen.

2. **Schutzziele der Massnahmen zur Gewährleistung der Datensicherheit als Minimalanforderungen definieren**
   Die Notwendigkeit der in Art. 2 E-VDSG aufgeführten technischen und organisatorischen Massnahmen hat sich nach den in Art. 1 E-VDSG vorgeschriebenen Grundsätzen zu richten. Die aufgeführten Schutzziele sind zu absolut und zu detailliert geregelt, so dass der Eindruck entsteht, dass es um absolut zu erreichende Anforderungen geht. Insofern werden statt Minimalanforderungen fälschlicherweise Maximalanforderungen formuliert. Die Bestimmung ist deshalb auf die Regelung der Schutzziele Integrität, Verfügbarkeit, Vertraulichkeit und Belastbarkeit zu reduzieren. Die Formulierung ist zudem in Bezug auf die Strafbarkeit von Verletzungen der Datensicherheit verfehlt, da die strafrechtlichen Anforderungen an die Bestimmtheit der strafbaren Tat nicht eingehalten werden.

3. **Pflicht zur Erstellung eines Bearbeitungsreglements streichen**
   Die Pflicht zur Erstellung eines Bearbeitungsreglements ist weitgehend deckungsgleich mit den Anforderungen an das zu erstellende Verzeichnis der Bearbeitungstätigkeiten. Dies produziert Rechtsunsicherheit und unnötigen Doppelaufwand. Art. 4 E-VDSG ist deshalb zu streichen.

4. **Keine Auferlegung von Pflichten gegenüber dem Auftragsdatenbearbeiter**
   Einzelne Pflichten des Verantwortlichen werden entgegen den Regelungen des revidierten Datenschutzgesetzes gleichzeitig dem Auftragsdatenbearbeiter auferlegt (etwa Art. 4 Abs. 1 E-VDSG und Art. 13 Abs. 1 E-VDSG) und setzen damit einen «Swiss Finish» zur EU-DSGVO. Dies ist zu korrigieren.

5. **Staatenliste des Bundesrates muss verbindlich sein**
   Die Staatenliste des Bundesrates (vgl. Art. 16 Abs. 1 des revidierten Datenschutzgesetzes und Art. 8 E-VDSG) muss für alle Akteure die Angemessenheit des Datenschutzes

verbindlich feststellen. Eine zusätzliche Einzelfallprüfung und die damit einhergehende Beurteilung einer ausländischen Rechtsordnung durch den Datenexporteur hinsichtlich hinreichender Transparenz und Rechtsschutz ist aus Praktikabilitätsgründen weder durchführbar noch zielführend.

6. **Korrektur der Aufgaben der Datenschutzberaterin bzw. des Datenschutzberaters**
   Die Datenschutzberaterin oder der Datenschutzberater hat die Aufgabe, die Verantwortliche Person betreffend die Datenschutzpflichten zu beraten. Eine Prüfung aller anfallenden Datenbearbeitungen kann damit nicht gemeint sein und wäre weder mit Blick auf die Anzahl möglich, noch aufgrund der Tatsache, dass nicht jede prüfenswerte Datenbearbeitung effektiv erkannt werden kann. Die Funktion Datenschutzberatung kann vielmehr nur solche Datenbearbeitungen prüfen, welche ihr effektiv vorgelegt werden. Dies ist in Art. 25 Abs. 1 Bst. a E-VDSG zu ergänzen.
   Die Regelung von Art. 25 Abs. 1 Bst. b E-VDSG widerspricht der oben beschriebenen Beratungsfunktion. Die Regelung kann zudem eine Verletzung aufsichtsrechtlicher Vorgaben zahlreicher regulierter Branchen mit hohem Grad an Arbeitsteilung mit sich bringen. Datenschutzberatung kann höchstens eine formelle Prüfung bedeuten im dem Sinne, dass aufgrund einer Selbstdeklaration Auskünfte von verantwortlichen Stellen eingeholt werden. Die tatsächliche Überprüfung der Funktionsweise und Qualität einer Datenbearbeitung wird eine Datenschutzberaterin oder ein Datenschutzberater nicht selbst durchführen können. Dies liegt in der Verantwortung der jeweiligen Verantwortlichen. Art. 25 Abs. 1 Bst. b E-VDSG ist deshalb zu streichen.

Wir bedanken uns für die wohlwollende Prüfung und Berücksichtigung unserer Anliegen. Für allfällige Rückfragen und weitere Erläuterungen stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Kantonalbanken

Hanspeter Hess
Direktor

Dr. Adrian Steiner
Vizedirektor
Leiter Public & Regulatory Affairs

VERBAND SCHWEIZERISCHER PRIVATSCHULEN VSP
FÉDÉRATION SUISSE DES ÉCOLES PRIVÉES FSEP
FEDERAZIONE SVIZZERA DELLE SCUOLE PRIVATE FSSP

Per E-Mail:

jonas.amstutz@bj.admin.ch

Bern, 14. Oktober 2021 Fi/jf

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) Stellung nehmen zu dürfen.

Der Verband Schweizerischer Privatschulen (VSP) vertritt auf nationaler Ebene die Interessen des Privatschulwesens. Betriebswirtschaftlich sind die Privatschulen überwiegend KMUs, die auf gute staatliche Rahmenbedingungen angewiesen sind. Wir sind daher für Lösungen, welche sich mit verhältnismässigem Aufwand umsetzen lassen und dabei auf die personellen und finanziellen Ressourcen der unterschiedlichen Schulen Rücksicht nimmt.

A. Das VDSG als Instrument zur Erreichung der Euro-Kompatibilität

Wie beim DSG hat der Bundesrat auch beim E-VDSG in seinen Erläuterungen festgehalten, dass es lediglich um die Angemessenheit des schweizerischen Datenschutzrechts im Vergleich zur europäischen DSGVO geht. In keiner Art und Weise wurde je von einer Erweiterung der Einschränkungen bei den Datenbearbeitungen bzw. von einer strengeren Regelung gesprochen. Diesem Ziel bleibt der Bundesrat auch bei der Formulierung der VDSG ausdrücklich verpflichtet. Alle Bestimmungen, welche folglich über die Erfordernisse der DSGVO hinausgehen, müssen als zweckfremd und als unzulässig abgelehnt werden. Diese sind konsequent aus dem E-VDSG zu löschen.

Verband Schweizerischer Privatschulen VSP
Hotelgasse 1
Postfach
3001 Bern

Tel. +41 31 328 40 50
Fax +41 31 328 40 55
info@swiss-schools.ch
www.swiss-schools.ch

B. Formelle Bemerkung

Zur besseren Lesbarkeit der Verordnung und zum klareren Bezug zum DSG würden wir klare Verweise auf die betroffenen Gesetzesbestimmungen im Titel der jeweiligen Bestimmungen begrüssen.

C. Zu den einzelnen Bestimmungen

Art. 1 Abs. 1 Bst. d

In Art. 1 Bst. d werden als Kriterium der Angemessenheit für die Datensicherheit die «Implementierungskosten» genannt. Es wird begrüsst, dass der Aufwand für die Verantwortlichen auch ausdrücklich in die Angemessenheitsüberprüfung aufgenommen wird. Der verwendete Begriff erscheint jedoch problematisch, da er lediglich auf die geldwerten Umsetzungsaufwendungen beschränkt werden könnte (siehe auch S. 16 der Erläuterungen). Für eine solche Einschränkung gibt es keinen Grund. Statt den Begriff «Implementierungskosten» schlagen wir vor, den allgemeineren Begriff «Aufwand für den Verantwortlichen» zu verwenden. Es gibt keinen Grund, beim Verantwortlichen überhöhte Planungs- oder Projektkosten auszulösen, nur um festzustellen, ob die Implementierung dann ihrerseits verhältnismässig ist.

Art. 1 Abs. 2

Diese Bestimmung verlangt die Überprüfung der technischen und organisatorischen Massnahmen in angemessenen Abständen (gemeint sind hier die zeitlichen Abstände). Aufgrund des risikobasierten Ansatzes der gesamten Thematik der Datensicherheit erscheint diese Regelung falsch. Zudem ist fraglich, ob mit der vom Bundesrat aufgestellten Forderung der Überprüfung in angemessenen Abständen die Delegationsnorm von Art. 8 Abs. 3 DSG eingehalten wird. Die Mindestanforderungen an die Datensicherheit rechtfertigen keine Einführung von zusätzlichen Kriterien, welche im Gesetz nicht verankert sind. Es ist - wenn überhaupt - in materieller Hinsicht zu fordern, dass ein Zusammenhang zwischen der Überprüfung der Datensicherheit und der Entwicklung des Risikos hergestellt wird.

➔ Formulierungsvorschlag: «Die Massnahmen sind bei einer relevanten Veränderung des Risikos zu überprüfen.»

Art. 2 Einleitungssatz

Die Bestimmung spricht von «Schutzzielen erreichen». Die Pannen der Swisscom zeigen mit aller Deutlichkeit auf: Die absolute Datensicherheit gibt es nicht. Von den Verantwortlichen zu verlangen, dass die entsprechenden Schutzziele erreicht werden, ist weder korrekt noch realistisch. Der Bereich der Datensicherheit ist ein typischer Bereich, bei welchem keine Ergebnisverantwortung, sondern nur eine Sorgfaltspflicht auferlegt werden darf.

➔ Formulierungsvorschlag: «Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele anstreben: (…)»

Nur so dürfen in der nachfolgenden Aufzählung Begriffe wie «verwehrt», «verunmöglicht», «verhindert», «gewährleistet», usw. überhaupt verwendet werden. Ansonsten müssten in der Aufzählung die Schutzziele jeweils vernünftig relativiert werden.

Art. 2 Bst. a bis k

Art. 2 dürfte eigentlich nur Schutzziele nennen, welche vom Verantwortlichen beeinflusst werden können. Gerade die Transportkontrolle kann beispielsweise durch viele externe Faktoren

gefährdet werden, für welche der Verantwortliche nicht einstehen kann. Die Aufzählung von Art. 2 Bst. a bis k zeigt, was in der Lehre verschiedentlich moniert worden ist: Mangels Effizienz der staatlichen Interventionen, wird die Last der «Privacy by design» vollumfänglich auf den Verantwortlichen abgewälzt, statt dass sie zu datenschutzfreundlichen Technologien durch die Hersteller von Hard- und Software führen würde. Diese Entwicklung zulasten der Nutzer von Informationstechnologien ist problematisch, da damit auch der Aufwand für die Datensicherheit dem Betreiber und nicht dem Entwickler von Informationstechnologien auferlegt wird. Die Aufzählung in Art. 2 Bst. a bis k ist in Beachtung dieser Problematik zu überarbeiten und dem Verantwortlichen dürfen nur Schutzziele auferlegt werden, die auch tatsächlich in seiner Verantwortung liegen.

Art. 3

Die nun in der Verordnung vorgesehenen Anforderungen an die Protokollierung übersteigen das vernünftige Mass und führen zu einer Bürokratie, welche in keinem Verhältnis zum tatsächlichen Nutzen der Anforderungen steht. Insbesondere die Aufbewahrungsdauer der Protokolle von 2 Jahren (Art. 3 Abs. 4 E-VDSG) ist unangemessen. Aus Sicht der Wirtschaft genügt die Pflicht zur Erstellung eines Verzeichnisses der Datenbearbeitungen vollumfänglich, um die Rechte und die Interessen der betroffenen Personen zu wahren.

Art. 4

Die Anforderungen von Art. 4 E-VDSG gehen zu weit. Ein Bearbeitungsreglement wird abgelehnt. Sollte wider Erwarten am Bearbeitungsreglement festgehalten werden, gibt es keinen nachvollziehbaren Grund zur «regelmässigen» Überarbeitung desselben. Dieses muss dann überarbeitet werden, wenn es einen Anlass zur Aktualisierung gibt (Veränderung der Bearbeitungsmittel oder Formen).

Art. 6 Abs. 1 und 2

Die Pflicht, für den Verantwortlichen, die vertrags- und gesetzesmässige Bearbeitung durch den Auftragsbearbeiter «sicherzustellen» ist konzeptionell falsch. Richtig ist, dass der Verantwortliche sich gemäss Art. 9 Abs. 2 DSG vergewissern muss, dass die Datenbearbeitung korrekt erfolgt. Diese unverhältnismässige, nicht einzuhaltende und nicht vom Gesetzgeber vorgesehene Verschärfung der Pflicht des Verantwortlichen ist im Rahmen der Delegation an den Bundesrat als zu weit gehend zu betrachten.

➔ Formulierungsvorschläge für Art. 6 Abs. 1 2. Satz bzw.
Art. 6 Abs. 2 2. Satz E-VDSG:
Er vergewissert sich, dass die Daten vertrags- und gesetzesgemäss bearbeitet werden. / Andernfalls muss er sich auf dem vertraglichen Weg vergewissern, dass ein gleichwertiger Datenschutz gewährleistet wird.

Art. 9 Abs. 2 und Art. 10 Abs. 1

Auch diese Forderung an den Verantwortlichen geht zu weit, wenn er «sicherstellen» muss. Der Terminus «vergewissern» ist zu verwenden.

Art. 15 und 16

Diese Bestimmungen finden keine Grundlage im DSG und sind ersatzlos zu streichen. Die Berichtigung, Löschung, Vernichtung oder Einschränkung der Bearbeitung von Personendaten (Art. 16 E-VDSG) erfolgen zudem im Interesse der betroffenen Person. Diese müssen ja so oder so den Anforderungen des Gesetzes entsprechen. Wieso in solchen Situationen eine neue Informationspflicht im Interesse der betroffenen Person liegen soll, ist nicht klar. Im

Gegenteil: Mit einer solchen Information, sei sie auch noch so klar, wird die betroffene Person oft verunsichert oder zumindest auf einen Umstand aufmerksam gemacht, der dazu führt, dass Fragen aufgeworfen werden und Aufwand generiert wird, der dem Verantwortlichen nicht entschädigt wird. Das wird von der Wirtschaft in nachvollziehbarer Weise als unnötige und bürokratische Zusatzbelastung empfunden. Auf unnötige Informationen ist in den Beziehungen zwischen dem Datenbearbeiter und der betroffenen Person zu verzichten.

Art. 18

Die Aufbewahrungsfrist von 2 Jahren nach Beendigung der Datenbearbeitung entbehrt einer gesetzlichen Grundlage im DSG und ist als zu lange zu betrachten. Die Aufbewahrung hat höchstens bis zur Beendigung der entsprechenden Datenbearbeitung zu dauern, da danach keine Verletzung der Rechte der betroffenen Person mehr erfolgen kann. Für die Frage, ob jemand durch die Datenbearbeitung ein Schutzrecht der betroffenen Person verletzt hat, ist nicht die Datenschutz-Folgenabschätzung relevant, sondern die konkrete Datenbearbeitung und die entsprechenden Verzeichnisse und Reglemente des Verantwortlichen.

Art. 19 Abs. 1 Bst. b bis d

Diese Kriterien sind dem Gesetz nicht zu entnehmen. Der Bundesrat hat weder eine Delegation noch eine Ermächtigung erhalten, Art. 24 DSG zu ergänzen. Deshalb sind diese Buchstaben aus der Verordnung zu streichen.

Art. 19 Abs. 1 Bst. e

Bei der Entdeckung einer Verletzung der Datensicherheit ist es eben gerade nicht immer möglich, die Folgen und die allfälligen Risiken umgehend und abschliessend festzustellen. Deshalb muss beim Bst. e «*soweit möglich*» vorangestellt werden.

Art. 19 Abs. 3

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 Abs. 4 DSG hinausgeht.

Art. 19 Abs. 5

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 24 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wider Erwarten an einer Dokumentationspflicht festhalten, sind die 3 Jahre deutlich zu lang. Eine Aufbewahrungsdauer soll höchstens ein Jahr betragen.

Art. 20 Abs. 5

Siehe die Bemerkung zu Art. 19 Abs. 1 Bst. b bis d E-VDSG. Auch hier hat der Bundesrat weder eine Delegation noch eine Ermächtigung erhalten, das DSG zu ergänzen. Deshalb ist dieser Absatz zu streichen, da er weit über Art. 25 DSG hinausgeht, der keine Dokumentationspflicht enthält. Sollte man wider Erwarten an einer Dokumentationspflicht festhalten, sind die 3 Jahre zu lang. Eine Aufbewahrungsdauer soll höchstens ein Jahr betragen.

Art. 22

Der Fristenlauf kann erst dann beginnen, wenn das Auskunftsgesuch formell korrekt eingereicht und inhaltlich klar ist. Solange das Gesuch entweder formell oder inhaltlich unklar ist,

kann die Frist nicht laufen. Dies muss im Art. 22 E-VDSG in aller Klarheit zum Ausdruck kommen.

Art. 23

Aufgrund der Einschränkungen, die gemäss Abs. 1 für die Kostenbeteiligung vom Bundesrat aufgestellt werden, steht der Betrag von CHF 300.00 in keiner vernünftigen Relation zum «unverhältnismässigen Aufwand». Bei Aufwendungen, die weit über CHF 1'000.00 gehen können, ist eine Kostenbeteiligung von nur gerade CHF 300.00 nicht angemessen. Natürlich hat der Verantwortliche die Kosten zu belegen. Aber es kann nicht sein, dass der Verantwortliche auf seinen Kosten sitzenbleibt und vom Kostenverursacher nur quasi ein symbolischer Betrag verlangt werden kann. Der Höchstbetrag ist deshalb anzuheben und sollte auf mindestens CHF 1'000.00 festgelegt werden.

Art. 24

Der Anspruch auf Datenportabilität bei der Datenherausgabe oder -übertragung, darf nicht ein absoluter sein. Dieser Anspruch darf nur bestehen, soweit die Bearbeitung von Personendaten in gängigen Formaten erfolgen kann bzw. erfolgt.

Art. 45 Abs. 1 und 2

Wenn die Kostenbeteiligung nach Art. 23 mit den Gebührengrundsätzen des EDÖB verglichen werden, dann muss von einer krassen Diskrepanz gesprochen werden. Der EDÖB erledigt eine Tätigkeit im Interesse der Bürger(innen) und der Volkswirtschaft Schweiz und es gibt keinen nachvollziehbaren Grund, weshalb die Person, welche Dienstleistungen von ihm in Anspruch nehmen muss, um sich datenschutzkonform zu verhalten, derart hohe Gebühren zu bezahlen hat. Weder kann es sein, dass die Gebühren nach Zeitaufwand berechnet werden (die Privatperson hat keinen Einfluss auf die Effizienz der Leistungserbringung durch den EDÖB), noch sind die Stundensätze von CHF 150.00 bis 350.00 angemessen. Diese Gebührenbestimmung stiftet die hilfesuchende Privatperson geradezu an, das Datenschutzrecht zu verletzen, da sie sich die Unterstützung durch den EDÖB nicht leisten kann. Die Gebührenordnung ist vollständig zu überdenken und auf ein vernünftiges Mass anzupassen. Hier wird dem Service-Public-Gedanken zu wenig Rechnung getragen. Es ist erforderlich, Maximalgebühren für Tätigkeiten festzulegen, welche der Einhaltung des Datenschutzrechts dienen (z.B. Art. 59 Abs. 1 Bst. c DSG, Konsultation aufgrund einer Datenschutz-Folgenabschätzung).

* *
*

Wir bitten Sie um Kenntnisnahme und danken für eine Berücksichtigung unserer Anliegen bestens.

Freundliche Grüsse

VERBAND SCHWEIZERISCHER PRIVATSCHULEN VSP

NR Dr. Gerhard Pfister
Präsident

Markus Fischer
Generalsekretär

VUD | Verein Unternehmens-Datenschutz

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik

Bundesrain 20, 3003 Bern

Zürich, den 14. September 2021

Sehr geehrte Damen und Herren

In der Beilage erhalten Sie die Vernehmlassung des Vereins Unternehmens-Datenschutz (www.vud.ch) zum Entwurf der Verordnung zum Datenschutzgesetz. Im VUD kommen die Datenschutzspezialisten zahlreicher Schweizer Unternehmen und bundesnaher Betriebe zusammen. Die Vernehmlassung wurde mit den Mitgliedern auf Basis ihrer Praxiserfahrung in der Umsetzung datenschutzrechtlicher Vorgaben in Unternehmen und der rechtlichen Rahmenbedingungen ausgearbeitet.

Zusammengefasst sind wir der Ansicht, dass manchen der Bestimmungen eine gesetzliche Grundlage fehlt und sie daher korrekterweise gestrichen werden müssen. Geschieht dies nicht, werden insbesondere bei den Bestimmungen zur Datensicherheit aufgrund der strafrechtlichen Sanktionierung erhebliche Unsicherheiten geschaffen, obwohl den meisten Bestimmungen die nach Art. 1 StGB erforderliche Bestimmtheit ohnehin fehlt. Überdies erachten wir manche der Bestimmungen leider als praxisfremd und in dieser Form nicht sinnvoll. Wir sind daher der Ansicht, dass der gegenwärtige Entwurf einer grundsätzlichen Überarbeitung bedarf.

Wir stehen für weitere Erläuterungen gerne zur Verfügung.

Freundliche Grüsse

David Rosenthal
Sekretär

Heribert Grab
Präsident

Verein Unternehmens-Datenschutz
c/o IT & Law Consulting GmbH,
Sternenstrasse 18, 8002 Zürich

www.vud.ch
info@itandlaw.ch
Tel.: +41 41 711 74 08

VUD Verein Unternehmens-Datenschutz

Vernehmlassung des VUD zum Entwurf der Verordnung zum revidierten DSG vom 23. Juni 2021

Streichungs- und Anpassungsvorschläge vom 13. September 2021

Vorbemerkungen:

- Zahlreichen Bestimmungen fehlt eine gesetzliche Grundlage[1] oder sie widersprechen gar direkt dem Willen des Gesetzgebers (insbesondere, was die an zahlreichen Stellen neu eingeführten Dokumentationspflichten betrifft). Sie sind daher zu streichen. Das gilt insbesondere im Bereich der Datensicherheit, deren Verletzung zu einer Strafbarkeit führen soll. Die Voraussetzungen hierfür sind in diesen Fällen jedoch nicht erfüllt, weshalb die Bestimmungen ins Leere schiessen.
- Die Verordnung sollte aus Sicht des VUD auf zu detaillierte Bestimmungen verzichten. Die Vielfalt der Bearbeitungsaktivitäten und Situationen ist so gross, dass Details in aller Regel mehr unbeabsichtigte negative Folgen haben als für Rechtssicherheit zu sorgen. Regelungen nach dem Giesskannenprinzip machen im Datenschutz schlicht keinen Sinn, sondern sind kontraproduktiv.
- Es sollten noch Übergangsfristen von 1 Jahr ab Inkrafttreten des revDSG für die Erstellung der Verzeichnisse und – falls darauf entgegen den Anträgen nicht verzichtet wird – auch für das Bearbeitungsreglement vorgesehen werden.
- Es wäre sinnvoll, bei den einzelnen Verordnungsbestimmungen jeweils auf den Artikel der revDSG verwiesen werden, um dessen Konkretisierung es geht.

Eine ausführlichere Fassung inklusive weiteren, erläuternden Bemerkungen zu den Regelungen des Entwurfs ist beim VUD erhältlich.

---

[1] «Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus (Art. 164 Abs. 2 BV). Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen (Art. 182 Abs. 2 BV). Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die **Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck.**» (BGE 141 II 169, E. 3.3).

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
1 Abs. 1	Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a. Zweck, Art, Umfang und Umstände der Datenbearbeitung; b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen; c. der Stand der Technik; d. Implementierungskosten.	Zu Abs. 1: Massnahmen zur Datensicherheit sind nicht «angemessen», sondern «geeignet», wie dies Art. 8 Abs. 1 revDSG auch sagt. «Angemessen» kann nur das resultierende Sicherheitsniveau sein. Man sollte deshalb auch in Art. 1 Abs. 1 von «geeigneten» Massnahmen sprechen, um terminologische Widersprüche zu vermeiden. Problematisch ist ferner, dass der Bundesrat von der falschen Vorstellung ausgeht, dass Art. 8 revDSG, der hier konkretisiert wird, mehr als die Datensicherheit i.e.S. regelt (CIA = Confidentiality, Integrity, Availability). Es geht weder um Bearbeitungsgrundsätze noch Betroffenenrechte. Die Beispiele in den Erläuterungen sind teilweise falsch. Ob z.B. eine Bearbeitung durch eine KI oder einen Menschen erfolgt, ist für die Frage der Datensicherheit nicht relevant. Ferner ist der Begriff des «Risikos» (Bst. b) falsch formuliert. Zudem geht es hier nicht um das Bruttorisiko, sondern das Nettorisiko. Der Begriff «Implementierungskosten» impliziert, dass anderer Aufwand nicht relevant ist. Das ist falsch. Ebenso falsch ist die Ausführung in der Erläuterung, dass übermässige Kosten nicht relevant sind. Erforderlich sind nur angemessene Massnahmen, und die Angemessenheit bestimmt sich selbst nach dem Vorschlag auch nach den Kosten.	Private Bundesorgane	Statt von «angemessenen» Massnahmen ist von «geeigneten» Massnahmen zu sprechen. Zu schreiben ist: «b. die verbleibenden potenziellen Auswirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit (Restrisiko).» «Implementierungskosten» ist durch «Implementierungsaufwand» zu ersetzen.
1 Abs. 2	Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.	Der Fokus auf die «angemessenen Abstände» ist zu eng. Wesentlich ist, dass sie in «angemessener Weise» überprüft werden. Der Begriff des «Abstands» impliziert nach wie vor eine Periodizität, die aber nicht zwingend ist, etwa wenn sich die Umstände nicht verändert haben.	Private Bundesorgane	Statt «angemessenen Abständen» ist «angemessener Weise» zu schreiben.
2	Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen: a. Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen.	Die Verwendung des Worts «erreichen» impliziert, dass die Schutzziele vollständig erfüllt werden, was weder erforderlich noch möglich ist. Zu treffen sind nur angemessene Massnahmen; eine vollständige Sicherheit ist nicht erforderlich. Die aufgeführte Liste ist überdies veraltet, zu absolut und zu detailliert formuliert. Zudem geht es grundsätzlich um die	Private Bundesorgane	Statt «erreichen» ist «anstreben» zu schreiben. Der Katalog der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	b. Zugangskontrolle: Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt. c. Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht. d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert. e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungs-systemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert. f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden. h. Bekanntgabekontrolle: Es kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden. i. Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden. j. Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des	Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. So ist es auch in Art. 32 Abs. 1 lit. b DSGVO definiert. Die Regelung zwingt zu einer Dokumentation für jede Datenbearbeitung (u.a. warum bestimmte der aufgeführten Schutzziele nicht relevant sind im konkreten Fall). Das widerspricht dem Willen des Gesetzgebers, der eine solche umfassende Dokumentationspflicht abgelehnt hat.		In diesem Fall wäre die Liste auch konform mit Art. 32 DSGVO.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	Systems beschädigt werden können (Dateninte-grität). k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.			
3 Abs. 1	Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.	Diese Bestimmung ist in mehrerlei Hinsicht problematisch und sollte ersatzlos gestrichen werden: *Erstens* fehlt ihr eine gesetzliche Grundlage. Es geht hier nicht primär um die Protokollierung zur Gewährleistung der Datensicherheit, sondern sie dient in erster Linie der *nachträglichen* Feststellung, ob es zu einer unbefugten Bearbeitung des Verantwortlichen bzw. seines Auftragsbearbeiters gekommen ist. Sollen unerlaubte Datenabflüsse, Malware, Einbrüche etc. entdeckt werden, sind andere Dinge zu protokollieren als die reguläre Nutzung der Daten (die Hacker und Malware vermeiden oder löschen werden). Zur Feststellung einer Verletzung der Datensicherheit eignet sie also nicht und ist damit unverhältnismässig. Art. 8 revDSG, welcher als Grundlage der Bestimmung dient, behandelt nur die Datensicherheit i.e.S. Nur solche sollte der Bundesrat gemäss Art. 8 Abs. 3 revDSG ausführen (und nur die Verletzung solcher können auch zu einer Strafbarkeit führen). *Zweitens* ist das Ergebnis der DSFA kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. In der Regel wird eine DSFA nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenbearbeitung. Dies hat jedoch mit Datensicherheit nichts zu tun. Die Erläuterungen des E-VDSG bestätigen sogar, dass es (auch) um die Gewährleistung der zweckkonformen Bearbeitung geht. *Drittens* muss eine solche Bearbeitung kraft Art. 21 revDSG ohnehin dem EDÖB oder Datenschutzberater vorgelegt werden. Eben dies dient bereits dem Ziel, eine solche oder andere Massnahme vorzuschlagen, soweit die Bearbeitung überhaupt	Private	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung erreicht das Ziel materiell nicht und zielt an der Sache vorbei.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		umgesetzt werden kann. Hier pauschal eine spezifische Massnahme ohne Berücksichtigung der Umstände vorzuschlage ist ein Schuss ins Blaue. *Viertens* obliegt die Pflicht auch dem Auftragsbearbeiter, der jedoch die DSFA nicht kennen muss und eine solche schon gar nicht auszuführen hat. Massnahmen zur Datensicherheit obliegen zwar auch ihm, aber diese Protokollierung ist in ihrem Kern keine solche. Das erklärt den unlösbaren Widerspruch. Auch deshalb ist sie zu streichen. Unklar ist aufgrund der Norm, ob eine Protokollierungspflicht auch dann bestehen soll, wenn eine Datenschutz-Folgenabschätzung unterlassen wurde, obwohl sie nötig gewesen wäre. Dies wird aber wohl so sein.		
3 Abs. 2	Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.	Die Pflicht zur Protokollierung besteht unabhängig vom Risiko und muss daher bei jeder automatisierten Bearbeitung von Personendaten vorgenommen werden. Der Begriff der automatisierten Bearbeitung ist nicht definiert. Zu verstehen ist darunter aber das Gegenteil zur manuellen Bearbeitung – somit ist darunter eine elektronische oder vergleichbare Datenbearbeitung zu verstehen. Die Protokollierungen erscheinen als unverhältnismässig – insbesondere, da auch das Lesen protokolliert werden muss. Auch im Falle von Bundesorganen ist die Regelung systematisch falsch und ohne gesetzliche Grundlage. Vgl. dazu die obigen Ausführungen.	Bundesorgan	Streichen (vgl. oben)
3 Abs. 3	Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.	Widerspruch zu den Mindestanforderungen an die Protokollierung gemäss den Absätzen 1 und 2. Abs. 3 bringt allerdings ebenfalls zum Ausdruck, dass es nicht um Verletzungen der Datensicherheit, sondern um etwaige unzulässige Bearbeitungen durch reguläre Benutzer geht. Diese stellen keine solche Verletzungen dar. Mit Empfänger ist die Organisation, nicht die Einzelperson gemeint.	Private Bundesorgane	Streichen (vgl. oben)

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
3 Abs. 4	Die Protokolle sind während zwei Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.	Für eine solche Aufbewahrungspflicht gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet, abgesehen vom Verzeichnis. Die Regelung der getrennten Aufbewahrung ist technisch nicht ohne Weiteres oder nur mit erheblichem Aufwand umsetzbar. Protokolle werden dort erzeugt, wo sie anfallen – und nicht auf anderen Systemen. Ein Betrieb müsste somit von sämtlichen Protokollen Kopien anfertigen und sie manuell auf ein anderes System übertragen; der Aufbewahrungsort muss ein unabhängiges System sein. Dieser Vorgang birgt seinerseits Sicherheitsrisiken, abgesehen davon, dass der Aufwand enorm wäre Es würde genügen, wenn sichergestellt wird, dass die Protokolle ihrerseits sicher sind. Die Personen, welche die Verletzung von Datenschutzvorschriften verfolgen, erhalten gemäss Wortlaut keinen Zugang zu den Daten. Die Zweckbindung ist unzulässig, da sie strenger ist, als die Bearbeitungsgrundsätze dies erlauben. Damit fehlt der Regelung eine gesetzliche Grundlage. Ein Verantwortlicher oder Auftragsbearbeiter hat möglicherweise ein Interesse, die Logs auch aus anderen Gründen auszuwerten. Tut er dies DSG-konform, sollte dies auch möglich sein. Die Regelung ist insofern interessant, als heute viele Protokolle von IT-Systemen aus Gründen des Datenschutzes weniger lang aufbewahrt werden. Es kann mit Verweis auf den E-VDSG vertreten werden, dass eine Aufbewahrung von zwei Jahren ohne Weiteres verhältnismässig ist, wenn sogar der Gesetzgeber diese Frist standardmässig vorschreiben will. Korrekterweise ist die Aufbewahrungsfrist aber als Mindestfrist auszugestalten. Gibt es Gründe, sie länger aufzubewahren, muss dies möglich sein.	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. «getrennt vom System, in welchem die Personendaten bearbeitet werden» ist zu streichen und durch «sicher» zu ersetzen. Die Regelung ist unverhältnismässig. Sofern eine Aufbewahrungsfrist überhaupt festgelegt wird, wofür es keine Grundlage gibt, so macht eine starre Frist keinen Sinn und wäre unverhältnismässig. Sie muss von der Dauer der Datenbearbeitung abhängig und generell angemessen sein. Satz 2 ist zu streichen, da er dem DSG widerspricht, indem er die Bearbeitungsgrundsätze aushebelt. Ohnehin müsste der Personenkreis mit Zugang ist um jene erweitert werden, welche die Verletzung von Datenschutzvorschriften verfolgen.
4 Abs. 1	Bearbeitungsreglement von privaten Personen 1 Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie:	Die Pflicht, für Datenbearbeitungen mit einem hohen Risiko Bearbeitungsreglemente zu erstellen, besteht bereits nach der geltenden Verordnung. Allerdings wurde allgemein erwartet, auch aufgrund der Botschaft des Bundesrats und der parla-	Private	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen.	mentarischen Beratung, dass die Bearbeitungsreglemente angesichts der neu eingeführten Dokumentations- und Informationspflichten (Verzeichnisse von Bearbeitungstätigkeiten, Datenschutz-Folgenabschätzungen, Datenschutzerklärungen) aus der Verordnung gestrichen werden. Das Bearbeitungsreglement dient augenscheinlich nicht der Sicherstellung der Datensicherheit i.e.S., sondern soll primär die Einhaltung der Bearbeitungsgrundsätze und die weiteren Vorgaben des Datenschutzes sicherstellen. Es fehlt der Bestimmung somit eine gesetzliche Grundlage, da Art. 8 revDSG nur Datensicherheit i.e.S. regelt. Der Vorgängernorm fehlt ebenfalls die gesetzliche Grundlage, weshalb sie toter Buchstabe blieb bzw. bleiben musste (ihre Verletzung hat keine Rechtsfolgen). Demgegenüber steht der enorme Aufwand, den die Erstellung und Nachführung eines solchen Bearbeitungsreglements mit sich bringt. Wie bei Abs. 2 gezeigt wird, werden die wesentlichen Angaben ohnehin bereits im Rahmen der in solchen Fällen erforderlichen Datenschutz-Folgenabschätzung dokumentiert, der Rest im ohnehin zu erstellenden Inventar. Die Regelung ist somit überflüssig. Auch die DSGVO sieht eine solche Regelung nicht vor (Swiss Finish). Während ein «Profiling mit hohem Risiko» in der Praxis vermutlich kaum vorkommen wird, stellt sich die Frage, ab wann «umfangreich» besonders schützenswerte Personendaten bearbeitet werden. Dies dürfte mit Bezug auf die HR-Daten bei einem mittleren und grösseren Umfang bereits der Fall sein. Auch jedes Medienunternehmen wird erfasst sein, welches Berichte über Politik und Gesellschaft enthält und damit auch besonders schützenswerte Personendaten (politische Ansichten etc.) bearbeitet. Es ist klar, dass besonders heikle Datenbearbeitungen eine betriebsinterne Regelung erfordern können. Dieser Aspekt ist jedoch über Art. 7 Abs. 1 revDSG bereits hinreichend geregelt.		ist unverhältnismässig und redundant. Es ist ein Swiss Finish.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Der Erläuterungsbericht suggeriert, dass das Bearbeitungsreglement ein in sich geschlossenes Dokument sein muss. Dies ist praxisfremd und unnötig. Eine solche Pflicht zur «Urkundeneinheit» gilt auch sonst nirgends. Es besteht ferner das Risiko, dass Auskunftsersuchende über die Generalklausel versuchen werden, an das Bearbeitungsreglement heranzukommen. Die Dokumentationspflichten wurden aus der DSGVO übernommen und zusätzlich soll diese bestehende Pflicht nicht gestrichen werden. Dies führt zu einer erheblichen Erweiterung der Dokumentationspflichten.		
4 Abs. 2	Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. zur internen Organisation; e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung,	Lit. a, b, c und f sind auch Bestandteile der Bearbeitungsverzeichnisse. Die übrigen Punkte müssen bei einer Datenschutz-Folgenabschätzung mitberücksichtigt werden, wenn diese für die Risikoabwägung bzw. als Massnahme zur Reduktion der Risiken relevant sind, was in der Regel der Fall sein wird. Somit sind sie bereits dokumentiert. Die Liste zeigt im Übrigen, dass es augenscheinlich primär nicht um Datensicherheit, sondern die Einhaltung der Bearbeitungsgrundsätze und des restlichen Datenschutzgesetzes geht (s. .	Private	Streichen (vgl. oben)

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.			
4 Abs. 3	Die private Person muss das Reglement regelmässig aktualisieren und der Daten-schutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.	Damit wird eine Pflicht zur Vorlage an den Datenschutzberater / die Datenschutzberaterin festgelegt, obwohl keine gesetzliche Verpflichtung besteht, diese Funktion überhaupt zu besetzen. Das Bearbeitungsreglement des Privaten muss weder publiziert noch dem EDÖB gemeldet werden.	Private	Streichen (vgl. oben). In jedem Fall den zweiten Halbsatz streichen.
5 Abs. 1	Das verantwortliche Bundesorgan und dessen Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie: a. besonders schützenswerte Personendaten bearbeiten; b. ein Profiling durchführen; c. Datenbearbeitungen im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG ausführen; d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen werden Personendaten zugänglich machen; e. Datenbestände miteinander verknüpfen; oder f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.	Aufgrund der Auflistung muss praktisch für jede automatisierte Bearbeitung ein Reglement erstellt werden. Es ist unklar, warum die Bearbeitungsreglemente trotz Einführung der Verzeichnisse und der Datenschutz-Folgenabschätzung beibehalten werden. Zudem fehlt aus den zu Art. 4 E-VDSG erwähnten Gründen eine gesetzliche Grundlage. Vgl. im Übrigen die obigen Ausführungen zu Art. 4 E-VDSG.	Bundesorgane	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung ist unverhältnismässig.
5 Abs. 2	Das Reglement muss mindestens die Angaben nach Artikel 4 Absatz 2 enthalten.	Die Formulierung ist unklar: Soll sie bedeuten, dass es allenfalls mehr Angaben enthalten muss?	Bundesorgane	Streichen (vgl. oben)

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
5 Abs. 3	Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen	Pflicht, das Bearbeitungsreglement dem Datenschutzberater und dem EDÖB bereitzustellen (auf Anfrage).	Bundesorgane	Streichen (vgl. oben)
6 Abs. 1	Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.	Der erste Satz wiederholt einerseits eine Banalität, ist andererseits aber ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall eingeschränkt ist, auch dann, wenn ihm nichts vorgeworfen werden kann. Dem ist nicht so. Es ist ohnehin nicht klar, was «für den Datenschutz verantwortlich» meint. Strafrechtliche Verantwortlichkeit kann es nicht sein, und aufsichtsrechtliche Verantwortlichkeit setzt ebenfalls Kontrollmöglichkeiten voraus. Wird die Verantwortlichkeit schliesslich als zivilrechtliche Haftung verstanden, dann wird mit dieser Regelung eine vom Gesetzgeber nicht vorgesehene Kausalhaftung eingeführt. Hierfür fehlt eine gesetzliche Grundlage. Dies würde auch über Art. 82 Abs. 3 DSGVO hinausgehen. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR. Die Formulierung «sicherstellen» ist zudem inhaltlich falsch. Der Verantwortliche kann nur «dafür Sorge tragen». Auch der zweite Satz ist mangelhaft, da ihm ebenfalls eine gesetzliche Grundlage fehlt. Nach Art. 9 Abs. 1 Bst. a revDSG hat der Verantwortliche zu sorgen, dass die Daten so bearbeitet werden, wie er es selbst darf. Nach Satz 2 hat er jedoch auch für die Durchsetzung seines eigenen Vertrags zu sorgen, selbst wenn dieser strenger sein sollte als das Gesetz. Macht er also einen zu strengen Vertrag, aber erlaubt er seinem Auftragsbearbeiter eine Bearbeitung, die noch dem Gesetz entspricht, ist diese Vorschrift bereits verletzt. Gemeint ist vielleicht auch eine Bezugnahme auf Art. 9 Abs. 1 DSG («… Bearbeitung … kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden…). Dies müsste in der Verordnung aber auch nicht wiederholt werden. Die Regel verwirrt also mehr als sie nutzt. Schon nach Art. 9 Abs. 1 Bst. a	Private Bundesorgane	Satz 1 streichen, da kein Mehrwert, jedoch verwirrend und falls als Kausalhaftung verstanden ohne gesetzliche Grundlage. Ohnehin ist «sicherstellen» durch «dafür Sorge tragen» zu ersetzen. Satz 2 streichen, da kein Mehrwert, jedoch verwirrend und ohne gesetzliche Grundlage, was die Pflicht zur Vertragsdurchsetzung betrifft.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		revDSG hat der Verantwortliche dafür zu sorgen, dass das DSG eingehalten wird. Das genügt.		
6 Abs. 2	Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.	Der Sinn und Zweck dieser Regelung erschliesst sich nicht, da der Regelungsgehalt bereits durch die Art. 16 und 17 revDSG (Bekanntgabe von Personendaten ins Ausland) gedeckt ist. Gemäss Erläuterungsbericht entspricht der neue Art. 6 Abs. 2 E-VDSG dem geltenden Art. 22 Abs. 3 VDSG. Dabei handelt es sich aber um eine Bestimmung für Bundesorgane, während Art. 6 Abs. 2 E-VDSG sowohl für Datenbearbeitungen Privater als auch für solche von Bundesorganen gelten soll. Aus dem Erläuterungsbericht geht nicht hervor, warum diese Bestimmung nun auch für Private gelten soll (oder warum es sie überhaupt braucht bzw. auf welche Rechtsgrundlage sie sich stützt). Die Regelung würde nur dort halbwegs Sinn machen, wo ein Schweizer Verantwortlicher einen ausländischen Auftragsbearbeiter bemüht Daten zu bearbeiten, ohne dass es zu einer Bekanntgabe aus der Schweiz kommt und somit Art. 16 revDSG nicht greift. Systematisch wäre aber auch dieser Fall in Art. 16 revDSG zu regeln und nicht in der VDSG. Es ist dies ein absoluter Sonderfall. Eine eigene Regelung in der VDSG rechtfechtfertigt sich dadurch nicht. Die Regelung ergibt sich im übrigen sowieso bereits aus Art. 9 Abs. 1 Bst. a revDSG, und zwar systematisch korrekt, während sie hier systematisch falsch angelegt ist: Im Falle einer Auftragsbearbeitung geht es um die Sicherstellung eines gleichwertigen Datenschutzes, da der Auftragsbearbeiter die Daten gar nicht in eigener Regie bearbeiten darf. Es geht darum sicherzustellen, dass die Daten nur so bearbeitet werden, wie der Verantwortliche dies darf – und so steht es schon in Art. 9 Abs. 1 Bst. a revDSG. Es ist allerdings zweifelhaft, ob die Autoren der Regelung diesen Sonderfall überhaupt im Blick hatten. Vermutlich wurde die Regel einfach übernommen, weil es sie schon gab.	Private Bundesorgane	Streichen. Die Regelung steht im Konflikt mit Art. 16 f. revDSG und Art. 9 Abs. 1 Bst. a revDSG, welche diesen Sachverhalt bereits abschliessend regeln.
6 Abs. 3	Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter	Gemäss den Erläuterungen zum E-VDSG schliesst die schriftliche Form auch die elektronische Form mit ein. Damit entspricht die Formulierung von Art. 28 Abs. 2 DSGVO, welche	Bundesorgane	Klarstellung, dass eine Genehmigung in Textform genügt und sie auch in allgemeiner Form

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich genehmigt hat.	ebenfalls «schriftlich» vorschreibt, damit aber auch den Fall des Nachweises durch Text meint. Es sollte ferner klargestellt werden, dass eine allgemeine Genehmigung (analog zur Regelung der DSGVO) zulässig ist, da es Bundesorganen sonst nicht möglich sein wird, Dienste von Standard-Online-Services zu beziehen. Diese verwenden ausschliesslich diese Methode.		erfolgen kann (beides analog DSGVO).
7	Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften entstehen.	Die Formulierung der Norm ist zu salopp. Es ist nicht klar, was «Probleme» sind. Die Norm stellt aber klar, dass Art. 28 Abs. 2 lit. a E-VDSG die Datenschutzberater*in *nicht* verpflichtet ist, *jede* Datenbearbeitung zu prüfen; andernfalls wäre eine Information bei Auftragsbearbeitungsverträgen a priori nicht erforderlich.	Bundesorgane	Satz 2 ist zu streichen, da unnötig. Jedenfalls ist er präziser zu formulieren.
9 Abs. 1	Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen mindestens die folgenden Punkte regeln: a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung und der Richtigkeit; b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen; c. die Art und der Zweck der Bekanntgabe von Personendaten; d. die Namen der Staaten, in die Personendaten bekanntgegeben werden; e. die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden; f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;	Die Aufzählung der Anforderungen an einen «Data Transfer Agreement» ist untauglich, weil sie nicht zwischen der Art der Übermittlung bzw. Rollen des Exporteurs und Importeurs unterscheidet. Diese sind jedoch für den Inhalt des Vertrags entscheidend, wie beispielsweise die vom EDÖB inzwischen anerkannten Standardvertragsklauseln der Europäischen Kommission (EU SCC) zeigen. So macht es keinen Sinn, einen Auftragsbearbeiter im Ausland zur Anwendung der Bearbeitungsgrundsätze, zur Information der betroffenen Personen oder zur Wahrung der Rechte der betroffenen Personen zu verpflichten. Sie müssten dem auch nach revDSG nicht nachkommen, weshalb nicht einzusehen ist, dass sie hierzu vertraglich verpflichtet werden sollen. In den Bearbeitungsgrundsätzen (Bst. a) fehlt der Grundsatz der Transparenz. Keine rechtliche Grundlage hat das Erfordernis in Bst. d und e, den Namen der Staaten oder der internationalen Organisationen zu nennen, denen Personendaten bekanntgegeben werden, soweit hiermit Weiterübermittlungen gemeint sind, was	Private Bundesorgane	Der Anforderungskatalog kann gestrichen werden, da der EDÖB sie sowieso prüfen muss. Wird dies nicht getan, ist der Anforderungskatalog entweder anzupassen, um unterschiedliche Konstellationen abzudecken (Controller, Processor) oder das «mindestens» ist durch «je nach den Umständen» zu ersetzen. Bst. a ist um den Grundsatz der Transparenz zu erweitern. Bst. d, e und f sind zu streichen.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger; h. die Massnahmen zur Gewährleistung der Datensicherheit; i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ; j. die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren; k. die Rechte der betroffenen Person, namentlich: 1. das Auskunftsrecht, 2. das Widerspruchsrecht, 3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten, 4. das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen.	nicht klar ist. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Auch die EU SCC beschränken sich darauf. Bst. f ist bereits mit dem Grundsatz der Verhältnismässigkeit abgedeckt und damit redundant. Bst. g geht zu weit, indem es die «berechtigten» Empfänger verlangt. Relevant sind die «Empfänger», also normalerweise die Parteien, welche den Vertrag abschliessen und damit bereits ersichtlich sind. Es fehlen Regelungen zur Meldung von Verletzungen der Datensicherheit, insbesondere soweit die betroffenen Personen zu informieren sind.		Meldungen betr. eine Verletzung der Datensicherheit sind zu regeln.
9 Abs. 2	Der Verantwortliche muss angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.	Der Begriff "sicherzustellen" impliziert eine Garantie der Einhaltung der Klauseln bzw. Kausalhaftung, wofür es keine gesetzliche Grundlage gibt und die vernünftigerweise auch nicht verlangt werden kann.	Private Bundesorgane	Der Begriff «sicherstellen» ist durch «in angemessener Weise Sorge zu tragen» zu ersetzen.
10 Abs. 1	Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.	Massnahmen sind angemessen, wenn sie dem Stand der Technik sowie den konkreten Umständen entsprechen. Die Anforderungen an die Massnahmen sind höher, wenn es sich beispielsweise um besonders schützenswerte Personendaten handelt. Wiederum kann der Exporteur nicht «sicherstellen», sondern nur dafür Sorge tragen. Der Erläuterungsbericht verlangt fälschlicherweise, dass der Empfänger verpflichtet werden muss, das Schweizer Datenschutzrecht einzuhalten. Das ist falsch. Einhalten muss er nur den Vertrag.	Private Bundesorgane	Der Begriff «sicherstellen» ist durch «in angemessener Weise Sorge zu tragen» zu ersetzen.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Die Vorschrift führt zu einer Kausalhaftung und ist in der Praxis nicht zu erfüllen. Nicht einmal das Bankenrecht kennt eine derart strenge Regelung. Zudem verlangen die aktuellen Standardvertragsklauseln, die in der Praxis flächendeckend eingesetzt werden, ohnehin entsprechende Sorgfaltspflichten des Exporteurs.		
12 Abs. 2	Der Verhaltenskodex enthält mindestens die Angaben nach Artikel 9 Absatz 1 und muss vorgängig vom EDÖB genehmigt werden.	Dies wird nicht möglich sein, da der Verhaltenskodex naturgemäss abstrakt und nicht für spezifische Unternehmen formuliert ist. Er wird somit beispielsweise die «Empfänger» (nicht: «Kategorien von Empfängern») nicht nennen. Dies ist jedoch gemäss dieser Bestimmung erforderlich. Ferner sollte nicht von «Angaben» die Rede sein, sondern von «Regelungen» oder «Punkten».	Private Bundesorgane	Der Verhaltenskodex «muss mindestens jene Punkte regeln, die nach dem Sinn und Zweck von Art. 9 Absatz 1 zu Regeln sind.»
13 Abs. 1	Der Verantwortliche und der Auftragsbearbeiter teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit.	Art. 13 Abs. 1 E-VDSG verweist auf eine Informationspflicht des Auftragsbearbeiters, was im Erläuterungsbericht auch nochmals ausdrücklich betont wird. Das revDSG sieht aber keine Informationspflicht des Auftragsbearbeiters vor, diese besteht gemäss Art. 19 revDSG (korrekterweise) nur für den Verantwortlichen. Da das Gesetz keine solche Pflicht für den Auftragsbearbeiter vorsieht, kann sie auch nicht über die Verordnung eingeführt werden. Art. 19 revDSG verlangt eine Information der betroffenen Personen, nicht eine Mitteilung. Für eine Information der betroffenen Person genügt ein Zugänglichmachen. Dies entspricht auch dem Verständnis unter der DSGVO. Es sollte durch die Wortwahl «mitteilen» keine Verschärfung impliziert werden. Stattdessen sollte analog zu den Informationspflichten im Finanzmarktrecht der Begriff «zur Verfügung stellen» verwendet werden. Das bringt auch besser zum Ausdruck, dass die Information ein Betroffenenrecht darstellt, dessen Ausübung eine gewisse Mitwirkung des Betroffenen verlangt. Die Erläuterungen erwähnen, dass eine Kommunikation über eine Website nicht immer genügt. Die Person müsse wissen, dass sie die Informationen auf einer bestimmten Website findet, und es wird z.B. für Telefongespräche nahegelegt, dass ihr der Link mündlich mitgeteilt wird. Solche Ausführungen sind	Private Bundesorgane	Die Erwähnung des Auftragsbearbeiters ist zu streichen. Es fehlt die gesetzliche Grundlage. Seine Erwähnung macht auch keinen Sinn. Es sollte nicht das Wort «mitteilen» verwendet werden, da es dafür keine gesetzliche Grundlage gibt. Korrekt wäre «Der Verantwortliche stellt die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form zur Verfügung.» Es sollte festgehalten werden, dass eine Information über eine Website in der Regel genügt.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		praxisfremd. Es sollte stattdessen festgehalten werden, dass die Information auf der Website genügt. Das entspricht der heutigen Praxis. Alles andere ist praxisfremd. Auch die Ausführungen in den Erläuterungen, wonach die betroffene Person die wichtigsten Informationen stets auf der ersten Kommunikationsstufe erhalten muss, ist schlicht falsch. Es gibt hierfür keine gesetzliche Grundlage, und es lässt jede Selbstverantwortung ausser Acht. Das ist auch deshalb bedenklich, weil der betroffenen Personen im Datenschutz eine Schlüsselrolle zukommt und es kontraproduktiv ist, ihr jede Eigeninitiative abzunehmen.		
13 Abs. 2	Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.	Werden Piktogramme verwendet, müssen diese maschinenlesbar sein. Letzteres soll gemäss dem Erläuterungsbericht einen Vergleich verschiedener Dokumente und allgemein eine gewisse Automatisierung ermöglichen – es stellt sich die Frage, inwieweit dies ein Ziel des Datenschutzes ist. Die Pflicht unterliegt auch einem Überlegungsfehler. Die Piktogramme haben den Zweck, den Menschen einfacher als über Text anzusprechen und ihm zu ermöglichen, intuitiv auf eine Datenschutzerklärung zu reagieren. Soll dagegen eine automatisierte Auswertung einer Datenschutzerklärung erfolgen, müsste die Datenschutzerklärung selbst, nicht die Piktogramme maschinenlesbar bzw. ihre Inhalte entsprechend codiert sein, und zwar unabhängig davon, wie sie optisch dargestellt ist. Bei der Maschinelesbarkeit geht es ja gerade *nicht* um die optische Darstellung. Abgesehen davon gibt es für eine solche Pflicht keine gesetzliche Grundlage. Die Verwendung von Piktogrammen ist freiwillig, und daher darf der Verwender auch entscheiden, ob sie maschinenlesbar sind oder nicht, was auch immer dies bedeutet. Schliesslich fehlt es auch an Standards für solche Angaben. Ohne Standards macht eine solche Regel keinen Sinn.	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. Die Regel macht auch keinen Sinn und führt im schlimmsten Fall zur Strafbarkeit. Dies kann wiederum dazu führen, dass keine Piktogramme verwendet werden.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
14	Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin.	Dies betrifft insbesondere die Statistik und Forschung. Die Regelung ist jedoch praxisfremd, denn es kann auch aus den Umständen hervorgehen, dass eine Auskunft freiwillig ist (Beispiel: Kundenzufriedenheitsumfrage eines Krankenversicherers)	Bundesorgane	Ergänzen mit «soweit dies nicht aus den Umständen ersichtlich ist»
15	Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.	Für diese «Informationspflicht bei der Bekanntgabe von Personendaten» gibt es keine gesetzliche Grundlage. Sie ist auch nach EU-Recht, auf welches sich der Erläuterungsbericht beruft, für private Datenbearbeiter nicht vorgeschrieben. Gegenüber der bisherigen Regelung in der VDSG wird die Vollständigkeit neu hinzugefügt, d.h. die Daten dürfen nicht lückenhaft sein. Die Regelung ist praxisfremd. Sie lässt sich nicht vernünftig umsetzen. Soll fortan jede E-Mail an eine andere Organisation einen entsprechenden Hinweis enthalten? Dazu kommt, dass der Empfänger ohnehin selbst verpflichtet ist, die Bearbeitungsgrundsätze einzuhalten und angemessene Massnahmen zu treffen, sich über die Richtigkeit der Daten zu vergewissern. Eine Information durch die übermittelnde Person unterläuft dies bzw. verabsolutiert eine der möglichen Vergewisserungsmassnahmen. Dies widerspricht dem Gesetz. Hinzu kommt, dass ein Auftragsbearbeiter etwas bekanntgeben soll, das er womöglich gar nicht hat.	Private Bundesorgane	Streichen, jedenfalls für private Datenbearbeiter. Es gibt keine gesetzliche Grundlage. Swiss Finish. Sie ist in dieser Form nicht praktikabel.
16	Der Verantwortliche informiert die Empfängerinnen und Empfänger, denen er Personendaten bekanntgegeben hat, unverzüglich über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten, ausser die Benachrichtigung ist unmöglich oder mit einem unverhältnismässigen Aufwand verbunden.	Die in Art. 16 E-VDSG vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren, war bereits im Entwurf des revDSG vorgesehen und wurde vom Parlament gestrichen. Die Einführung dieser Pflicht über die revidierte Verordnung würde daher dem Willen des Parlaments widersprechen. Dieselbe Bestimmung verweist zudem auf ein Recht auf Einschränkung der Bearbeitung von Personendaten, das so im revDSG nicht besteht.	Private Bundesorgane	Streichen. Es gibt keine gesetzliche Grundlage.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Die Regelung erwähnt zudem die «Einschränkung» der Bearbeitung. Dies spielt auf Art. 18 DSGVO an, welche Bestimmung in der Schweiz so nicht existiert.		
18	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.	Für eine solche Aufbewahrungspflicht gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet, abgesehen vom Verzeichnis. Die Regelung geht ferner davon aus, dass eine Datenschutz-Folgenabschätzung nie erneuert wird. Dies entspricht jedoch nicht der Praxis. Es ist nicht klar, wie mit mehreren Datenschutz-Folgenabschätzungen umzugehen ist.	Private / Bundesorgane	Klarstellen: «… muss in der aktuellsten Fassung während zwei Jahren …» Die Aufbewahrungspflicht ist zu streichen. Es fehlt eine gesetzliche Grundlage. So oder so ist sie als Mindestfrist auszugestalten. Es ist klarzustellen, dass Schriftlich «in Textform» meint.
19 Abs. 1	Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit: a. die Art der Verletzung; b. soweit möglich den Zeitpunkt und die Dauer; c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten; d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen; e. die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen; f. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder die Folgen zu mildern; g. den Namen und die Kontaktdaten einer Ansprechperson.	Bst. e ist falsch formuliert. Die «allfälligen Risiken» beinhalten bereits die Folgen für die betroffenen Personen. Richtig müsste es heissen «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht». Auch in Bst. f müsste nicht von den «Folgen», sondern vom «Risiko» die Rede sein. Gemildert werden kann entweder das Schadensausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem «Risiko» entspricht). Gemäss den Erläuterungen wird das in Art. 24 Abs. 2 revDSG erwähnte «voraussichtlich» so interpretiert, dass auch dann gemeldet werden muss, wenn das Vorliegen eines «hohen Risikos» nicht ausgeschlossen werden kann. Diese Aussage hilft nicht weiter, da es sich um einen Pleonasmus handelt. Der Begriff «Risiko» beinhaltet bereits eine Wahrscheinlichkeitsüberlegung, d.h. wie wahrscheinlich es ist, dass ein Schaden eintritt. Es bleibt dabei: Die Wahrscheinlichkeit muss eine gewisse Höhe aufweisen.Wünschenswert wäre schliesslich eine «de minimis»-Regelung, die jene Fälle ausschliesst, in welchen der EDÖB ohnehin nicht wirklich etwas tun kann oder will, obwohl ein hohes Risiko vorliegt (z.B. eine problematische E-Mail geht an den falschen Empfänger und ein Missbrauch durch diesen ist möglich). Damit können auch die Ressourcen des EDÖB	Private Bundesorgane	Im Einleitungssatz ist aufzunehmen: «… bei einer meldepflichtigen Verletzung …» Bst. e ist umzuformulieren: «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht» Es sollte eine «de minimis»-Regelung vorgesehen werden, in welchen trotz eines hohen Risikos für eine betroffene Person nicht gemeldet werden muss. Bst. f. sollte angepasst werden: "gegebenenfalls welche Massnahmen getroffen wurden …"

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		geschont werden, die er für andere, für den Datenschutz wichtigere Angelegenheiten einsetzen kann.		
19 Abs. 2	Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.	Der Hinweis «bei Entdeckung der Verletzung der Datensicherheit» erscheint wenig sinnvoll. Zu diesem Zeitpunkt wird der Verantwortliche nie über alle Informationen verfügen, da sich diese immer erst über Zeit herausstellen. Der Hinweis kann ersatzlos gestrichen werden.		Streichung von «bei Entdeckung der Verletzung der Datensicherheit»
19 Abs. 5	Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.	Eine Dokumentationspflicht kennt zwar die DSGVO. Das revDSG sieht sie jedoch nicht vor. Daher kann sie und die entsprechende Aufbewahrungspflicht auch nicht auf dem Weg der Verordnung eingeführt werden. Noch die Botschaft zum revDSG hielt fest, dass keine allgemeine Dokumentationspflicht eingeführt werden soll. Genau dies wird hier (und in anderen Bestimmungen) durch die Hintertür versucht. Es bleibt jedenfalls unklar, wozu die Dokumentations- und Aufbewahrungspflicht dient, ausser allenfalls dem EDÖB. Da sich aus der Systematik aber ergibt, dass ohnehin nur meldepflichtige Verletzungen zu dokumentieren sind, erschliesst sich auch dieser Sinn nicht wirklich: Ist gemeldet und interessiert sich der EDÖB dafür, wird er sofort nachfragen. Tut er dies nicht, wird er kaum später darauf zurückkommen. Der Hinweis auf alle «zusammenhängenden Tatsachen» ist falsch, denn er suggeriert, dass Tatsachen nur für die Dokumentationspflicht erforscht werden müssen, was sicherlich nicht erforderlich ist. Warum hier drei statt wie sonst zwei Jahre vorgesehen sind, ist unklar.	Private Bundesorgane	Streichen. Es fehlt die gesetzliche Grundlage. Die Norm ist auch nicht nötig. Der Begriff «Tatsachen» ist durch «und dokumentierten Tatsachen» zu präzisieren.
20 Abs. 3	Die Auskunft muss für die betroffene Person verständlich sein.	Sie muss verständlich sein. Ob die betroffene Person sie im konkreten Fall versteht, ist nicht relevant. Beim Auskunftsbegehren geht es darum, die bearbeiteten Daten mitzuteilen. Müssen diese noch so erläutert werden, dass	Private Bundesorgane	Den Begriff «für die betroffene Person» streichen. Statt «verständlich» soll «im Grundsatz nachvollziehbar

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		sie für die betroffene Person verständlich sind, kann dies zu einem unverhältnismässigen Aufwand führen. Das Auskunftsrecht bietet Zugang zu Daten, nicht ein Recht darauf, die Datenbearbeitung so lange erklärt zu bekommen, bis sie die jeweilige Person versteht. Eine solche Pflicht hat keine Grundlage im Gesetz. Beispielsweise können die im Rahmen einer klinischen Studie bearbeiteten Daten oder technische Logdaten für die betroffene Person unverständlich sein. Müssen diese zuerst so dargestellt werden, dass sie für die betroffene Person verständlich sind, sind aufwändige Erläuterungen erforderlich, mitunter auch sehr viel Fachwissen. Abgesehen davon, dass dies nicht unbedingt innerhalb von 30 Tagen erfolgen kann, sprengt dies jeden Rahmen und ist unverhältnismässig. Nirgends in Europa wird das Auskunftsrecht so verstanden.		sein, sofern damit kein unverhältnismässiger Aufwand verbunden ist» verwendet werden. Eine Alternative wäre folgende Formulierung: «Die Auskunft darf nicht irreführend sein.»
20 Abs. 4	Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.	Es fehlt eine gesetzliche Grundlage für eine echte Verpflichtung der betroffenen Person. Insofern macht Satz 2 wenig Sinn. Lässt sich die Identität der betroffenen Person nicht verifizieren, erhält sie auch keine Auskunft.	Private Bundesorgane	Begriff «Identifizierung» ersetzen durch den Begriff «Authentifizierung»
20 Abs. 5	Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.	Diese Dokumentation kann bspw. durch eine Kopie des Antwortschreibens erreicht werden. Bei einer mündlichen Auskunft müsste daher z.B. eine Telefonnotiz erstellt werden. Das revDSG sieht keine solche Dokumentations- und Aufbewahrungspflicht vor. Sie kann nicht auf dem Verordnungsweg eingeführt werden. Sie ist auch wenig sinnvoll. Sie zwingt den Verantwortlichen, Personendaten entsprechend länger aufzubewahren bzw. mehr Personendaten zu beantworten, als er dies womöglich tun würde. Die betroffene Person erhält eine Antwort auf ihr Ersuchen. Will sie dagegen vorgehen, kann sie diese Antwort ins Recht legen. Die Bestimmung sorgt nur für zusätzlichen Aufwand. Wie sich die drei Jahre herleiten, ist unklar.	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. Die Bestimmung bietet keinen Mehrwert, sorgt aber für zusätzlichen Aufwand.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
21 Abs. 1	Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.	Unklar ist, welche Rechtsfolge die «Unzuständigkeit» eines Verantwortlich hat.	Private Bundesorgane	Es ist zu präzisieren: "Sind für die Bearbeitung von Personendaten mehrere gemeinsam verantwortlich …"
21 Abs. 2	Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen.	Diese Bestimmung ist verwirrlich, da sie impliziert, dass der Auftragsbearbeiter selbst eine Auskunftspflicht hat, wenn er faktisch in der Lage sein sollte, eine Auskunft zu erteilen bzw. er das Auskunftsgesuch in einem solchen Fall nicht weiterleiten muss, auch wenn er es nicht beantwortet. Das kann nicht sein. Die Regelung sollte präzisiert werden.	Private Bundesorgane	Am Ende sollte es heissen: «sofern er das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet.»
22 Abs. 1	Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen.	Die Frist kann erst dann zu laufen beginnen, wenn das Begehren klar und die betroffene Person korrekt identifiziert ist. Dies ist sie zu Beginn häufig nicht.	Private Bundesorgane	Zu präzisieren: «… seit dem Vorliegen eines klaren Begehrens und der korrekten Identifikation der betroffenen Person.»
23 Abs. 2	Die Beteiligung beträgt maximal 300 Franken.	Der Betrag wird nicht verändert, weil es seit seiner Einführung zu keiner relevanten Teuerung gekommen sei und der Betrag nicht abschreckend sein soll. Allerdings steht dieser Kostendeckel im Vergleich zum Aufwand, den ein Auskunftsersuchen trotz entsprechender Strukturen mit sich bringen kann, in keinem Verhältnis (z.B. können umfassende Schwärzungen erforderlich sein, was Kosten pro Fall von CHF 10'000 mit sich bringen kann). Auch die DSGVO kennt keine betragsmässige Begrenzung, sondern verlangt, dass er «angemessen» ist. Auch im Öffentlichkeitsrecht kann eine Gebühr verlangt werden. Der Betrag soll durchaus abschreckend sein, weil er die betroffenen Personen dahingehend diszipliniert, Auskunftsersuchen nur dann zu stellen, wenn sie wirklich angezeigt sind und nicht aus Jux.	Private Bundesorgane	Betrag den Verhältnissen anpassen (mindestens CHF 3'000) Alternativ ist die Bestimmung zu streichen, da die angemessene Kostenbeteiligung bereits in Abs. 1 enthalten ist. Beispiel: Aufwand bis CHF 500 trägt das Unternehmen, darüber hinaus müssen die Kosten zu 50% übernommen werden.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
23 Abs. 3	Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen.	Es ist zu präzisieren, dass die Antwortfrist von 30 Tagen erst danach beginnt.	Private Bundesorgane	Präzisieren: «Erst danach beginnt die Frist zur Beantwortung des Auskunftsbegehrens.»
25	Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen muss folgende Aufgaben wahrnehmen: a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden. b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.	Es ist schon konzeptionell nicht richtig, dass der Datenschutzberater die Aufgaben «wahrnehmen» muss, er muss sie «haben». Zu lit. a: Die breite der Prüfpflicht geht am Ziel vorbei, als sie impliziert, dass der Datenschutzberater im Grund kein Berater mehr ist, sondern als "Datenschutzpolizist" agieren sollte, d.h. alles und jeden in Bezug auf den Datenschutz zu überprüfen. Richtig wäre stattdessen, dass seine beratende Funktion betont wird, und zwar dort, wo ihn die verantwortlichen Stellen beiziehen wollen. Das ist auch das Prinzip, das der Gesetzgeber bei der DSFA verfolgt: Wenn der Verantwortliche die DSFA nicht dem EDÖB vorlegen will, was er kann, dann kann er sie stattdessen dem Berater vorlegen. So sieht es auch Art. 10 Abs. 2 Bst. a revDSG vor. Dem ist hier Rechnung zu tragen. Der Berater sollte nur auf Beizug aktiv werden. Abgesehen davon ist beim bestehenden Vorschlag unklar, in welchem Umfang die Bearbeitungen zu prüfen sind (alle, einige, nur die ihm vorgelegten, nur nach Risiko) und welche Folgen es hat, wenn der Datenschutzberater dieser Aufgabe nicht nachkommt. Die Erläuterungen implizieren, dass alle Bearbeitungsaktivitäten überprüft werden müssen, was nicht richtig sein kann. Auch hier kann risikoorientiert geprüft werden. Zu lit. b: Nur das Vorlegen der DSFA dem/der DSB genügt nicht, der/die DBS muss bei der Erstellung der DSFA mitwirken. Dabei müssen die Risikobewertung und vorgeschlagenen Massnahmen geprüft werden.	Private	Die Bestimmung sollte gestrichen werden, da im Gesetz bereits alles nötig gesagt wird. Sie stammt noch aus einer Zeit, in welcher das Gesetz noch keine solchen Ausführungen enthielt. Wird sie beibehalten, ist sie zu präzisieren: «Der Datenschutzberaterin oder dem Datenschutzberater eines privaten Verantwortlichen müssen folgende Aufgaben übertragen worden sein:» Bst. a ist anzupassen: "Wo sie oder er beigezogen wird, prüft sie oder er die Bearbeitung …"
26	Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind	Unternehmen mit weniger als 250 Mitarbeitenden (wohl nicht FTE) müssen folglich nur diejenigen Bearbeitungstätigkeiten in Verzeichnissen dokumentieren, die die genannten Kriterien erfüllen, d.h. eine Datenbearbeitung durchführen, die ein hohes Risiko mit sich bringt.	Private	Es ist klarzustellen, dass wenn eine der beiden Voraussetzungen erfüllt ist, die Verzeichnis-

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.	Unklar ist, ab wann «umfangreich» besonders schützenswerte Personendaten bearbeitet werden. Genügt die Bearbeitung von HR-Daten? Sind die Voraussetzungen für die Befreiung nicht erfüllt, ist das Verzeichnis für alle Bearbeitungsaktivitäten zu führen. Dies impliziert jedenfalls der Wortlaut der Bestimmung. Art. 12 Abs. 5 revDSG erlaubt die Ausnahme nur, wenn ein «geringes Risiko» vorliegt. Demnach ist der Bundesrat der Auffassung, dass wenn weder Bst. a noch b erfüllt ist, per se ein geringes Risiko vorliegt. Das würde den Anwendungsbereich von Art. 22 revDSG (DSFA) stark einschränken. Zudem ist darauf hinzuweisen, dass diese Ausnahme bei Art. 3 und 4 nicht vorgesehen ist, was zu absurden Folgen führt. Generell sollten für Verzeichnisse Übergangsfristen vorgesehen werden, da sie einen sehr hohen Aufwand mit sich bringen.		pflicht nur für die entsprechenden Bearbeitungen mit hohem Risiko gelten. Der Begriff der Mitarbeitenden ist durch "Vollzeitstellen" zu ersetzen. Es ist eine Übergangsfrist zur Umsetzung der Verzeichnispflicht von einem Jahr vorzusehen.
31	Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von Personendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden.	Es ist unklar, was «sogleich» bedeuten soll. Es muss genügen, dass die Erfordernisse des Datenschutzes im Projekt rechtzeitig berücksichtigt werden.	Bundesorgane	Der Begriff «sogleich» ist durch «rechtzeitig» zu ersetzen.
32 Abs. 1	Das verantwortliche Bundesorgan meldet dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung. Der EDÖB nimmt diese Meldung in das Register der Bearbeitungstätigkeiten auf.	Bereits geplante automatisierte Bearbeitungstätigkeiten müssen gemeldet werden, was zu einem erheblichen Mehraufwand für die Dokumentation führt. Zudem muss jede geplante automatisierte Bearbeitung gemeldet werden, nicht nur solche mit einem (potenziellen) hohen Risiko. Die Meldung muss im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung erfolgen. Diese erfolgen oft auf der Basis eines vorgegebenen Rahmens, während die konkreten Entscheidungen erst im Verlauf des Projekts getroffen	Bundesorgane	Streichen, es fehlt die gesetzliche Grundlage. Zudem liegen die zu meldenden Informationen im Zeitpunkt, in dem die Meldung erfolgen soll, in der Regel nicht in der genügenden Detailtiefe vor. Die Ressourcenplanung des EDÖB rechtfertigt zudem nicht den mit dieser frühen Meldung

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		werden. Daraus folgt, dass die verlangten Angaben in dem Zeitpunkt in der Regel noch nicht in der genügenden Detailtiefe vorliegen werden. Zudem sollte sich gemäss Botschaft zu Art. 11 Abs. 4 E-DSG (Art. 12 Abs. 4 revDSG) keine Änderung im Vergleich zum bestehenden Recht ergeben. Eine Pflicht, geplante Datensammlungen dem EDÖB zu melden, besteht aber nach geltendem Recht nicht. Es fehlt daher an einer gesetzlichen Grundlage. Gemäss Erläuterungsbericht dient die frühe Meldung zudem nicht dem Persönlichkeitsschutz, sondern der Ressourcenplanung des EDÖB. Art. 47 E-VDSG enthält eine Übergansbestimmung für automatisierte Bearbeitungstätigkeiten, die bei Inkrafttreten des E-VDSG bereits produktiv sind. Diese Übergangsbestimmung ist insofern keine Erleichterung, als für bereits produktive Bearbeitungen ein Verzeichnis erstellt und dieses an den EDÖB gemeldet werden muss.		einhergehenden Mehraufwand der Bundesbehörden.

Autoren: Maria Winkler (Basisdokument, Kommentierung), David Rosenthal (Kommentierung, Anpassungsvorschläge), David Vasella (Anpassungsvorschläge). Berücksichtigt wurde auch die Kommentierung von David Vasella (https://datenrecht.ch/zum-entwurf-der-revidierten-vdsg-eine-verpasste-chance/ und https://datenrecht.ch/taeglich-gruesst-das-murmeltier-gedanken-zum-vorentwurf-der-datenschutzverordnung/)). Ferner wurden die Bemerkungen und Kommentare der Mitglieder des VUD anlässlich der Fachsitzung vom 1. September 2021 verarbeitet.

walderwyss rechtsanwälte

Walder Wyss AG
Seefeldstrasse 123
Postfach
8034 Zürich
Schweiz

Telefon +41 58 658 58 58
Telefax +41 58 658 59 59
www.walderwyss.com

Per E-Mail an jonas.amstutz@bj.admin.ch

Frau Bundesrätin Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

David Vasella
Partner
Dr. iur., CIPP/E, CIPM
Rechtsanwalt
Direkt +41 58 658 52 87
david.vasella@walderwyss.com

Jürg Schneider
Partner
Dr. iur., Rechtsanwalt
Direkt +41 58 658 55 71
juerg.schneider@walderwyss.com

Zürich, 14. Oktober 2021

Stellungnahme zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Der Bundesrat hat im Juni 2021 die Vernehmlassung zum Entwurf der Verordnung zum Bundesgesetz über den Datenschutz (nachfolgend «**E-VDSG**») eröffnet und zur Stellungnahme bis zum 14. Oktober 2021 eingeladen.

Walder Wyss AG ist eine der grössten Wirtschaftskanzleien der Schweiz. Als solche beraten wir im Bereich des Datenschutzes und verwandter Gebiete Unternehmen aller Branchen und Grössen ebenso wie öffentliche Organe. Wir begleiten das Datenschutzrecht auch publizistisch, z.B. auf dem Blog http://datenrecht.ch. Wir haben uns dort bereits kritisch zum E-VDSG geäussert.[1]

Vor diesem Hintergrund nehmen wir die Gelegenheit zur Stellungnahme zum E-VDSG gerne wahr. Zusammenfassend können wir folgendes festhalten:

– Es ist richtig, den Datenschutz zu stärken, wie dies die Revision des DSG und in ihrem Zuge auch der VDSG verfolgt. Der Formalismus, das Misstrauen gegenüber den Verantwortlichen und die Vernachlässigung der Eigenverantwortung der Betroffenen, wie dies im E-VDSG deutlich zum Ausdruck kommt, diskreditiert den Datenschutz aber und erreicht das Gegenteil.

1 https://datenrecht.ch/zum-entwurf-der-revidierten-vdsg-eine-verpasste-chance/.

- Diverse Bestimmungen der E-VDSG haben keine gesetzliche Grundlage, weder im revidierten DSG noch anderswo.
- Diverse Bestimmungen des E-VDSG führen zu Mehraufwand, der zum geringen Nutzen im keinem Verhältnis steht.

Wir beschränken uns im Folgenden auf Kernpunkte und schliessen uns im Übrigen der Stellungnahme des Vereins Unternehmens-Datenschutz (**VUD**) an.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Mit freundlichen Grüssen,

David Vasella Jürg Schneider

1. Kapitel, 1. Abschnitt: Datensicherheit (Art. 1-5)

Art./Abs.	Bemerkungen	Formulierungsvorschlag
Art. 1 Abs. 2	Für die Beurteilung der Angemessenheit auf eine Periodizität der Beurteilung abzustellen ist falsch. Eine Überprüfung ist bspw. nicht erforderlich, wenn sich die Umstände seit der letzten Beurteilung nicht verändert haben. Es obliegt dem Verantwortlichen und dem Auftragsbearbeiter, die Angemessenheit der Massnahmen so und dann zu prüfen, wie es die Umstände verlangen.	Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in ~~angemessenen Abständen~~ angemessener Weise zu überprüfen.
Art. 2	Art. 2 gestaltet die Schutzziele als Minimalanforderungen aus, die in jedem Zeitpunkt der Datenbearbeitung erfüllt sein müssen. Oft ist aber nicht jedes Schutzziel relevant. Auch ein Nullrisiko nicht möglich und nicht gefordert (Art. 8 Abs. 1 revDSG: «angemessener» Datensicherheit). Massnahmen müssen bestimmte Ziele deshalb nicht «erreichen».	~~Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen:~~ Die Massnahmen zur Gewährleistung der Datensicherheit müssen in angemessener Weise auf die folgenden Schutzziele hinwirken: […]
Art. 3	Art. 3 Abs. 1: — Es fehlt eine gesetzliche Grundlage. — Eine Datenschutzfolgenabschätzung ist ungeeignet zur Feststellung, ob die Datensicherheit verletzt oder besonders gefährdet ist. — Eine Protokollierungspflicht widerspricht dem Willen des Gesetzgebers, der keine Accountability i.S.d. DSGVO wollte. — Die Protokollierungspflicht obläge hier auch dem Auftragsdatenbearbeiter. Dieser muss aber weder eine Datenschutzfolgenabschätzung vornehmen noch jene des Verantwortlichen kennen. Art. 3 Abs. 2: Zudem fehlt eine gesetzliche Grundlage. Eine «automatisierten Bearbeitung» wird zudem praktisch jede Bearbeitung erfassen. Art. 3 Abs. 2 statuiert daher eine allgemeine Protokollierungspflicht. Das ist unverhältnismässig. Art. 3 Abs. 3: Art. 3 Abs. 3 konkretisiert die Protokollierungspflicht von Art. 3 Abs. 1 und Abs. 2 E-VDSG, verlangt aber mehr als diese Bestimmungen. Sie steht daher im Widerspruch zu ihnen. Zudem fehlt ihr eine gesetzliche Grundlage. Art. 3 Abs. 4: Es fehlt eine gesetzliche Grundlage. Zudem wäre eine getrennte Aufbewahrung der Protokolle enorm aufwendig.	Streichen.

Art. 4	Art. 4 ist mangels gesetzlicher Grundlage ersatzlos zu streichen. Systematisch wird das Bearbeitungsreglement für private Personen zwar im Abschnitt der Datensicherheit geregelt, doch es handelt sich nicht um eine Mindestanforderung an die Datensicherheit (Art. 8 Abs. 3 revDSG). Zur Dokumentation genügt gemäss der Botschaft zum revDSG das Bearbeitungsverzeichnis, dessen Inhalt sich mit jenem des Reglements überschneidet. Art. 4 Abs. 3 suggeriert ferner, dass immer eine Datenschutzberaterin oder ein Datenschutzberater zu bestellen wäre. Das ist bei Privaten gemäss dem revDSG aber optional.	Streichen.
Art. 5	Dieser Bestimmung fehlt eine gesetzliche Grundlage. Es kann auf die Ausführungen zu Art. 4 Abs. 1 verwiesen werden. Zudem müsste im Ergebnis für praktisch jede Bearbeitung ein Bearbeitungsreglement erstellt werden. Die Dokumentationspflichten des revDSG stellen ohnehin bereits sicher, dass Bearbeitungstätigkeiten aufgezeichnet werden. Art. 5 Abs. 1 ist unnötig und unverhältnismässig.	Streichen.

1. Kapitel, 2. Abschnitt: Bearbeitung durch Auftragsbearbeiter (Art. 6-7)

Art./Abs.	Anliegen und Begründung	Formulierungsvorschlag
Art. 6 Abs. 1	Art. 6 Abs. 1 suggeriert eine uneingeschränkte Verantwortlichkeit des Verantwortlichen, der einen Auftragsbearbeiter beizieht. Das ist rechtsdogmatisch falsch. Zudem fehlt Art. 6 Abs. 1 Satz 2 eine gesetzliche Grundlage. Der Verantwortliche muss nach Art. 9 Abs. 1 lit. a DSG Sorge tragen, dass der Auftragsbearbeiter Daten nicht in einer Weise bearbeiten darf, die dem Verantwortlichen nicht erlaubt wäre; nicht mehr und nicht weniger. Diese Bestimmung genügt, trägt aber gleichzeitig nicht die weitergehende Pflicht nach Art. 6 Abs. 1 Satz 2 revDSG.	Streichen.

1. Kapitel, 3. Abschnitt: Bekanntgabe von Personendaten ins Ausland (Art. 8-12)

Art./Abs.	Anliegen und Begründung	Formulierungsvorschlag
Art. 9 Abs. 1	Es fehlen gerade diejenigen Inhalte, die für eine Übermittlung von Personendaten in Länder ohne angemessenes Datenschutzniveau zentral sind. Dies sind insbesondere Vereinbarungen, in welcher Form lokale Rechtsvorschriften geprüft	Neu einfügen: “die Pflicht der Parteien, die lokalen Rechtsvorschriften in Bezug auf die

	oder berücksichtigt werden und wie im Fall von Behördenzugriffen zu verfahren ist. Überflüssig ist die Präzisierung in lit. g in Bezug auf die "zur Bearbeitung der Daten berechtigten" Empfänger, da ein entsprechender Vertrag notwendigerweise nur berechtigte Empfänger aufführt. Für eine generelle Informationspflicht des Empfängers gegenüber der betroffenen Person gemäss lit. j gibt es keine Grundlage.	Datenbekannte zu prüfen und zu überwachen;" Neu einfügen: "die Pflichten des Empfängers im Fall des Zugangs von Behörden zu Personendaten;" Streichen in lit. g: "~~zur Bearbeitung der Daten berechtigten~~" Lit. j streichen.
Art. 10	In Bezug auf die Standarddatenschutzklauseln der EU-Kommission ist diese Bestimmung mittlerweile überflüssig, da Entsprechendes bereits aus Art. 14 und 15 der Standarddatenschutzklauseln folgt. Zudem kann der Datenexporteur nicht "sicherstellen", dass der Empfänger die Klauseln beachtet, sondern den Empfänger nur entsprechend vertraglich verpflichten und die Einhaltung dieser Pflichten überprüfen. Auch dies folgt jedoch bereits aus den Standardvertragsklauseln sowie den dazu erlassenen Auslegungshilfen.	Streichen.

2. Kapitel: Pflichten der Verantwortlichen und des Auftragsbearbeiters und (Art. 13-19)

Art./Abs.	Anliegen und Begründung	Formulierungsvorschlag
13 Abs. 1	Die Pflicht des *Auftragsbearbeiters* zur Information hat keine gesetzliche Grundlage. Art. 19 revDSG statuiert richtigerweise nur eine Pflicht des Verantwortlichen zur Information. «In präziser, verständlicher und leicht zugänglicher Form» ist angesichts des Transparenzerfordernisses überflüssig. Zudem genügt grundsätzlich der Hinweis auf eine Datenschutzerklärung auf einer Website oder im Menü einer App. Vom Betroffenen kann erwartet werden, die entsprechenden Informationen aufzurufen. Die Informationspflicht von Art. 19 DSG verlangt keine rechtsgeschäftliche Mitteilung, sondern eher eine Deklaration der Bearbeitungen analog dem, was das Konsumenteninformationsgesetz vorsieht. Es genügt daher die Abrufbarkeit der entsprechenden Angaben. Auch widerspricht der Erläuternde Bericht der allgemeinen Praxis, wenn er sagt, eine Kommunikation über eine Webseite genüge nicht immer (vgl. S. 30). Es ist Standard, die geforderten Informationen auf dem Internetauftritt des Verantwortlichen bereitzustellen. Betroffene wissen das und gehen	1 Der Verantwortliche ~~und der Auftragsbearbeiter teilen~~ stellt diejenigen ~~die~~ Informationen, die zur Erfüllung seiner Informationspflicht erforderlich sind, in angemessener Art und Weise zur Verfügung. ~~über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit.~~ 1bis (neu) Der Verantwortliche weist die betroffene Person erforderlichenfalls darauf hin, wo sie die erforderlichen Informationen einsehen kann.

	davon aus, Datenschutzinformationen auf der Internetseite des Verantwortlichen zu finden. Der Besuch einer Internetseite ist heute problemlos zumutbar, wie steigenden Nutzerzahlen belegen, ebenso wie der Umstand, dass die Amtliche Sammlung des Bundes-rechts primär im Internet veröffentlicht wird (Art. 1a PublG).	
13 Abs. 2	Diese Bestimmung wurde unbesehen aus Erwägungsgrund 60 der DSGVO übernommen. Die Verwendung von Piktogrammen in Datenschutzerklärungen ist wünschenswert. Wird Maschinenlesbarkeit gefordert, werden Verantwortliche aber auf Piktogramme verzichten. Auch besteht für eine Maschinenlesbarkeit kein erkennbares und vor allem kein datenschutzrechtlich motiviertes Bedürfnis.	Streichen.
Art. 14	In vielen Fällen ist bereits aufgrund der Umstände offensichtlich, dass eine Auskunft freiwillig ist.	Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin, soweit dies nicht aus den Umständen ersichtlich ist.
Art. 18	Die Folgenabschätzung muss nicht ausgedruckt und unterschrieben werden ist. Dafür fehlen eine gesetzliche Grundlage und jedes Bedürfnis. Es genügt, die Folgenabschätzung so festzuhalten, dass ein Nachweis durch Text möglich ist. Für eine Aufbewahrungspflicht fehlt zudem eine gesetzliche Grundlage. Ohnehin liegt es im Interesse des Verantwortlichen, die Datenschutzfolgenabschätzungen nachweisen zu können.	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in anderer Form, die einen Nachweis mittels Text erlaubt, festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Daten-bearbeitung aufbewahrt werden.~~ Sie muss in der jeweils aktuellen Fassung während mindestens zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.
Art. 19 Abs. 5	Es fehlt eine gesetzliche Grundlage für eine Dokumentationspflicht im Sinne von Art. 19 Abs. 5. Sie dient auch nur dem EDÖB, der bereits nach Art. 19 Abs. 1 informiert wird. Schwammig ist zudem der Hinweis auf alle «zusammenhängenden Tatsachen», und es ist offen, weshalb in Art. 19 Abs. 5 eine dreijährige – und nicht z.B. zweijährige –	Streichen.

	Aufbewahrungsfrist statuiert wird; ohnehin ist eine Aufbewahrungspflicht aber unnötig.	

3. Kapitel: Rechte der betroffenen Person (Art. 20-24)

Art./Abs.	Anliegen und Begründung	Formulierungsvorschlag
Art. 20 Abs. 3	Der E-VDSG zeigt auch hier, wie wenig er den Betroffenen zutraut. Es reicht, wenn eine Auskunft als solche verständlich ist; ob der konkrete Betroffene sie versteht, ist nicht Sache des Verantwortlichen, der auf Sonderbedürfnisse keine Rücksicht nehmen muss.	Streichen.
Art. 20 Abs. 5	Das revDSG enthält keine gesetzliche Grundlage für Art. 20 Abs. 5. Zudem liegt es ohnehin im Interesse des Verantwortlichen, die Gründe für die Verweigerung, die Einschränkung oder den Aufschub zu dokumentieren und erhält die betroffene Person nach Art. 20 Abs. 2 eine begründete Antwort, was den Zweck von Art. 20 Abs. 5 erfüllt.	Streichen.
Art. 22 Abs. 1	Die Antwortfrist darf erst beginnen, wenn die betroffene Person identifiziert ist das Begehren ausreichend klar ist, was eine Präzisierung verlangen kann. Ein früherer Fristbeginn führt nur zu einer standardmässigen Berufung auf die Verlängerungsmöglichkeit nach Art. 22 Abs. 2, was auch dem Betroffenen nicht dient.	Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen. Die Frist beginnt mit der Identifizierung und ggf. der Präzisierung des Begehrens durch den Betroffenen.
Art. 23 Abs. 2	Auskunftsbegehren werden in der Praxis häufig missbraucht. Eine Kostenbeteiligung von CHF 300 steht dazu und zum Aufwand des Verantwortlichen in keinem Verhältnis. Wird diese Schwelle nicht erheblich erhöht, kann sich der Verantwortliche bei besonderem Aufwand auf Rechtsmissbräuchlichkeit des Begehrens (Fallgruppe des krassen Missverhältnisses der Interessen) berufen.	Die Beteiligung beträgt maximal 5'000 Franken.
Art. 23 Abs. 3	Selbsterklärend.	Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen. Die Auskunftsfrist beginnt frühestens mit Ablauf dieser Frist.

5. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane (Art. 27-36)

Art./Abs.	Anliegen und Begründung	Formulierungsvorschlag
Art. 29 Abs. 2	Aus Gründen des Persönlichkeitsschutzes muss der Name des Datenschutzberaters nicht publiziert werden. Es genügt eine funktionsbezogene E-Mail-Adresse.	Es veröffentlicht ~~die Kontaktdaten~~ eine E-Mail-Adresse der Datenschutzberaterin oder des Datenschutzberaters im Internet und teilt ~~diese~~ dem EDÖB die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters mit.
Art. 32	Es fehlt eine gesetzliche Grundlage für eine Meldepflicht nach Abs. 1. Sie wäre zudem unverhältnismässig. Es wären faktisch alle Bearbeitungstätigkeiten zu melden. Unklar ist aber schon, wann eine Bearbeitung «geplant» ist. Die Meldung müsste aber zu einem Zeitpunkt erfolgen, bei dem die erforderlichen Informationen noch gar nicht abschliessend vorliegen. Auch kann der EDÖB mit diesen Informationen nichts anfangen; es fehlen ihm schon die Ressourcen, sie weiterzuverfolgen.	Streichen.