Verordnung über die Informationsverwaltung und -sicherheit (VO IVS)

(vom …)

Vernehmlassungsvorlage, Version 4,
5. Dezember 2016

Der Regierungsrat,

gestützt auf das Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007 und das Archivgesetz vom 24. September 1995

beschliesst:

		Erläuterungen
	A. Geltungsbereich	
	§ 1. Diese Verordnung regelt die Verwaltung und den Schutz von Informationen der öffentlichen Organe von Kanton und Gemeinden.	*Die Verordnung präzisiert die Grundzüge über die Informationsverwaltung und -sicherheit, die namentlich in den §§ 5 und 7 des Gesetzes über die Information und den Datenschutz (IDG) vorgegeben sind. Soweit es die Informations-verwaltung der kantonalen Verwaltung betrifft, bildet § 5 Abs. 4 IDG die rechtliche Grundlage. Für die übrigen öffentlichen Organe ergibt sich diese aus den allgemeinen Bestimmungen des IDG.* *Informationen öffentlicher Organe durchlaufen in ihrem Lebenszyklus drei Phasen:* *1. Phase: laufende Dossiers zu laufenden Geschäftsfällen* *2. Phase: abgeschlossene Dossiers während der Aufbewahrungsfrist* *3. Phase: archivierte Dossiers* *Die vorliegende Verordnung regelt die ersten beiden Phasen von der Eröffnung eines Dossiers*

		bis zu dessen Abschluss, die Aufbewahrung in der Ruhenden Ablage während der Aufbewahrungsfrist und schliesslich die Anbietungspflicht an das Archiv. Die dritte Phase ist in der Archivverordnung geregelt.
	B. Dossierführung und Ordnungssystem	
Dossierbildung	§ 2. [1] Das öffentliche Organ legt alle für die Bearbeitung und die Nachvollziehbarkeit eines Geschäftsfalls notwendigen Informationen in einem Dossier ab. [2] Auf Informationen, die aus technischen, organisatorischen oder rechtlichen Gründen separat abgelegt werden, wird im Dossier verwiesen.	*Insbesondere um das Transparenzprinzip gemäss § 4 IDG zu erfüllen sowie die Nachvollziehbarkeit des Verwaltungshandelns und die Rechenschaftsfähigkeit gemäss § 5 Abs. 1 IDG zu gewährleisten, sind alle Informationen zu einem Geschäftsfall in einem Dossier zu führen. Es darf keine Informationen geben, die ohne Zuordnung zu einem Dossier geführt werden. Ausgenommen sind Dokumente ohne direkte Relevanz für einen Geschäftsfall, beispielsweise Unterlagen von kurzfristiger Bedeutung (Informationen für den gleichen Tag) oder Schreiben Dritter, die lediglich zur Kenntnis genommen werden.* *Zur Zuverlässigkeit von Informationen gehört, dass relevante Geschäftsvorgänge aufgezeichnet werden. So sind beispielsweise nur mündlich besprochene Vorgänge, die über den Tag hinaus von Bedeutung sind, in Form von Protokollen oder Telefonnotizen schriftlich festzuhalten.* *Neben den üblichen Geschäftsfällen (z. B. Rekursfälle, Bewilligungen usw.) sind auch Projekte, Objekte, Prozesse oder bestimmte Aufgaben als Geschäftsfälle zu betrachten. Entsprechend werden beispielsweise Dossiers zu IT-Projekten, zu Liegenschaften oder Betrieben geführt.* *Aus verschiedenen Gründen müssen bestimmte*

		Informationen separat, also ausserhalb des Dossiers, abgelegt werden, beispielsweise: • *Spezialformate: separate Ablagen für audio-visuelle Medien oder für Überformate (z. B. grossformatige Pläne)* • *Informationen oder Unterlagen in Fachan-wendungen (z. B. SAP)* • *handunterzeichnete Dokumente oder Original-urkunden, die zwecks Rechtsgültigkeit auf Papier aufbewahrt werden müssen.* *Solche separat abgelegten Dokumente sind im Dossier zu vermerken oder es sind Geschäfts-regeln zu formulieren, die die generelle Nachvoll-ziehbarkeit von (Standard-)Geschäften gewähr-leisten.*
Federführung	§ 3. Das öffentliche Organ bezeichnet pro Geschäftsfall eine federführende Stelle. Diese ist für die Vollständigkeit des Dossiers verantwortlich.	*Diese Festlegung entlastet weitere an einem Geschäftsfall mitarbeitende Personen von der Dossierführung. Sie können allenfalls vorhandene Informationen zu einem Geschäftsfall jederzeit vernichten, weil sie durch die Festlegung der Federführung wissen, wer das vollständige Dossier führt.* *Arbeiten mehrere öffentliche Organe zusammen (z. B. in Projekten), ist jedes Organ selber dafür verantwortlich, dass der eigene Beitrag zum gesamten Geschäftsfall nachvollziehbar und rechenschaftsfähig dokumentiert ist. Das heisst, dass neben dem federführenden Organ, welches das Hauptdossier führt, die mitarbeitenden Organe jeweils eigene Dossiers zum gleichen Geschäftsfall führen, in denen beispielsweise interne Meinungs-bildungsprozesse oder die Erarbeitung von Grund-*

		lagen dokumentiert sind. *Wenn mehrere Organe am gleichen Geschäftsfall beteiligt sind und ein gemeinsames Dossier führen (z. B. auf einer Kollaborationsplattform), muss mindestens eines der beteiligten Organe zur Führung des massgeblichen Dossiers verpflichtet werden.*
Metadaten	§ 4. Dossiers werden mit Informationen versehen, die für die Bearbeitung und die Zuordnung eines Geschäftsfalls nötig sind (Metadaten). Metadaten sind insbesondere Titel des Geschäftsfalls, Eröffnungs- und Abschlussdatum sowie federführende Stelle.	*Neben technischen Metadaten, die beispielsweise von Informationsverwaltungssystemen automatisch vergeben werden, sind inhaltliche Metadaten als beschreibende Merkmale für die systematische und effiziente Bewirtschaftung der Dossiers wichtig. Entsprechend kann die Vergabe von Metadaten – mit Ausnahme der im Erlasstext genannten – nicht generell abstrakt festgelegt werden. Sie wird vielmehr von jedem öffentlichen Organ gemäss seinen Aufgaben und Organisationsstrukturen geregelt. Weitere Metadaten können beispielsweise das Aktenzeichen, die Position im Ordnungssystem, den Status eines Geschäftsfalls, Zugangsbestimmungen (sofern diese für das ganze Dossier gleich sind) oder Aufbewahrungsfristen betreffen.*
Dossierabschluss	§ 5. [1] Ist ein Geschäftsfall beendet, überprüft die federführende Stelle die Vollständigkeit des entsprechenden Dossiers und schliesst es ab. [2] Informationen, die für die Nachvollziehbarkeit eines Geschäftsfalls nicht notwendig sind, werden entfernt.	*Für die Bewirtschaftung eines Dossiers ist dessen Abschluss essentiell. Ab diesem Zeitpunkt beginnt die Aufbewahrungsfrist zu laufen (vgl. z. B. § 5 Abs. 2 IDG), nach deren Ablauf die öffentlichen Organe ihre Informationen dem zuständigen Archiv zur Bewertung anbieten müssen.* *Beim Abschluss soll noch einmal die Vollständigkeit des Dossiers überprüft werden, damit die Nachvollziehbarkeit des Geschäftsfalls gewährleistet werden kann. Gleichzeitig werden für die*

		Nachvollziehbarkeit des Geschäftsfalls nicht mehr relevante Informationen aus dem Dossier entfernt und sachgerecht vernichtet.
Ordnungssystem	§ 6. Das öffentliche Organ verwaltet seine Dossiers mit einem Ordnungssystem, das eine eindeutige Zuordnung und eine zielgerichtete Suche von Informationen ermöglicht.	*Ein Ordnungssystem (bisher in § 8 Abs. 4 Archivverordnung „Registraturplan“ genannt) ist eine zumeist hierarchische, aufgabenorientierte Struktur, die für alle vorkommenden Geschäftsfälle eine geeignete Ablageposition zur Verfügung stellt. Es erlaubt:* • *eine zielgerichtete, strukturierte Suche,* • *die genaue Zuordnung von Informationen zum jeweiligen Dossier (keine Mehrfachablagen),* • *die einfache Bewirtschaftung von Metadaten,* • *die langfristige Erhaltung des Entstehungs- und Verwendungszusammenhangs von Informationen* • *und die einheitliche Verwaltung unterschiedlicher Informationsträger.* *Auf der Basis von Geschäftsregeln und zusammen mit den Metadaten wird das Ordnungssystem zu einem eigentlichen Managementsystem für die Informationsverwaltung. Der Detaillierungsgrad des Ordnungssystems ist dem jeweiligen öffentlichen Organ und der Anzahl seiner Aufgaben anzupassen.* *Jedes neue Dossier wird bei seiner Eröffnung einer geeigneten Position im Ordnungssystem zugeordnet.*

	C. Informationsträger	
Wahl des Informationsträgers	§ 7. [1] Das öffentliche Organ legt fest, ob es Dossiers entweder in physischer (insbesondere auf Papier) oder in elektronischer Form führt. Es kann Ausnahmen festlegen. [2] Es legt zudem fest: a. wie bei der physischen Dossierführung mit elektronischen Informationen verfahren wird, b. wie bei der elektronischen Dossierführung mit physischen Informationen verfahren wird.	*Das öffentliche Organ legt in einem Grundsatzentscheid die massgebliche Form seiner Dossiers fest. Eine möglichst grosse Einheitlichkeit der gewählten Informationsträger (physisch oder elektronisch) reduziert Doppelspurigkeiten und erleichtert die Bewirtschaftung der Dossiers.* *Ausnahmen können für bestimmte Dokumente oder ganze Dossiertypen festgelegt werden, beispielsweise für grossformatige Pläne, die nur schwer eingescannt werden können, oder für umfangreiche Excel-Tabellen, die sich kaum in einer sinnvollen Form ausdrucken lassen. Bestimmte Dokumente (z. B. handunterzeichnete Dokumente und andere Originalurkunden) sind zwecks Rechtsgültigkeit zusätzlich zur elektronischen Version weiterhin physisch zu führen und aufzubewahren. Für bestimmte Dokumenttypen gibt es rechtliche Vorgaben betreffend die Wahl des Informationsträgers.* *Bei grundsätzlich physischer Dossierführung muss festgelegt werden, wie mit in elektronischer Form vorliegenden Informationen verfahren wird (beispielsweise dass diese ausgedruckt und im Dossier abgelegt werden müssen).* *Bei grundsätzlich elektronischer Dossierführung muss insbesondere festgelegt werden, wie mit in physischer Form vorliegenden Informationen verfahren wird (beispielsweise dass diese eingescannt bzw. auf eine andere Art digitalisiert werden müssen oder dass im elektronischen Dossier zumindest auf den physischen Ablageort verwie-*

		sen werden muss). Es muss sichergestellt sein, dass alle für die Nachvollziehbarkeit eines Geschäftsfalls relevanten Dokumente in elektronischer Form im Dossier abgelegt werden. Für die tägliche Arbeit (z. B. an Sitzungen) wird es (zumindest vorläufig) weiterhin auch physische Doppel der im elektronischen Dossier abgelegten Dokumente geben. Diese müssen aber jederzeit ohne Informationsverlust vernichtet werden können und schliesslich – spätestens nach Abschluss des Geschäfts – tatsächlich auch datenschutzkonform vernichtet werden.
Einführung neuer technischer Mittel	§ 8. [1] Bei der Einführung neuer technischer Mittel, insbesondere neuer Informationsverwaltungssysteme, stellt das öffentliche Organ sicher, dass die vorhandenen Informationen und Metadaten verwendbar bleiben. [2] Neue technische Mittel gewährleisten, dass ein Export der Informationen in archivtauglichen Formaten möglich ist.	*Werden neue technische Mittel zur Verwaltung von Informationen (beispielsweise elektronische Geschäftsverwaltungssysteme oder Fachanwendungen) eingeführt, müssen die in den Vorgängeranwendungen vorhandenen Informationen entweder vollständig übernommen werden können, oder es ist auf andere Art dafür zu sorgen, dass die Informationen samt Metadaten verwendbar bleiben, bis sie dem zuständigen Archiv zur Bewertung und allfälligen Übernahme angeboten werden können. Das Gleiche gilt auch für technische Mittel im physischen Bereich: so muss etwa gewährleistet sein, dass ein Film oder eine Tonbildschau abgespielt werden kann, bis diese zur Archivierung angeboten werden können.* *Werden neue elektronische Systeme eingeführt, sind sie mit einer archivischen Ablieferungsschnittstelle auszurüsten, die einen strukturierten Export der Informationen in archivtauglichen Formaten erlaubt. Für die Kantonsverwaltung wurde mit RRB Nr. 538/2014 die Schnittstelle gemäss Standard eCH-0160 verbindlich erklärt.*

		Verfügt eine Verwaltungseinheit über Dossiers mit einer Aufbewahrungsfrist von mehr als zehn Jahren, ist ein Datenexport in archivtaugliche Formate bereits vor der Archivierung angezeigt, um die Informationen lesbar zu halten.
	D. Anbietungspflicht und Archivierung	
Anbietungspflicht	§ 9. [1] Das öffentliche Organ sondert Dossiers, deren Aufbewahrungsfristen abgelaufen sind, regelmässig aus und bietet sie zusammen mit den dazugehörigen Metadaten dem zuständigen Archiv an. Es liefert die vom Archiv ausgewählten Dossiers ab. [2] Fällt eine öffentliche Aufgabe dahin, bietet das bislang für die Aufgabenerfüllung zuständige Organ seine Dossiers zusammen mit den dazugehörigen Metadaten dem zuständigen Archiv an. [3] Vom Archiv nicht übernommene Dossiers sowie Doppel der ans Archiv abgelieferten Informationen werden vernichtet oder unwiederbringlich gelöscht. [4] Archivwürdige Dossiers, die vom Archiv aus Kapazitätsgründen nicht sofort übernommen werden können, bewahrt das öffentliche Organ weiter auf.	*Die vorliegenden Regelungen werden von § 10 Archivverordnung hierher überführt, weil sie den Abschluss der Informationsverwaltung der öffentlichen Organe betreffen und noch nicht die Archivierung.* *Abs. 1: Sofern es keine spezialrechtlichen Bestimmungen gibt, richten sich die Aufbewahrungsfristen nach § 5 Abs. 2 IDG und § 8 Abs. 1 Archivgesetz und betragen maximal zehn Jahre. Alle Dossiers, deren Aufbewahrungsfristen abgelaufen sind, werden dem zuständigen Archiv samt den dazugehörigen Metadaten (Verzeichnissen, Registerdaten, Geschäftskontrolldaten usw.) angeboten. Das Archiv bewertet diese gemäss § 8 Abs. 2 Archivgesetz und § 6 Archivverordnung auf ihre Archivwürdigkeit hin. Die öffentlichen Organe sorgen für den Transport der archivwürdigen Dossiers und Metadaten ins zuständige Archiv.* *Abs. 2: Ersetzt § 10 Abs. 2 Archivverordnung. Gemäss IDG §§ 3 (Definition „öffentliche Organe“) und 5 Abs. 3 müssen Informationen erst dann nicht mehr zur Archivierung angeboten werden, wenn die öffentliche Aufgabe selbst ins Privatrecht überführt oder ganz aufgegeben wird, also dann wenn der Staat die Verantwortung für die Aufgabenerfüllung aufgibt. Hingegen bleibt die Anbie-*

		tungspflicht bestehen, wenn eine öffentliche Aufgabe neu einer privatrechtlich organisierten Körperschaft übertragen wird oder wenn das mit der Erfüllung der öffentlichen Aufgabe betraute Organ ins Zivilrecht überführt wird, ohne dass auch die eigentliche Aufgabe materiell privatisiert wird. *Abs. 3: Gemäss § 5 Abs. 3 IDG sind angebotene Informationen, die vom zuständigen Archiv nicht übernommen werden, vom öffentlichen Organ unwiederbringlich zu vernichten. In physischer Form vorliegende Informationen sind zu schreddern oder auf andere Art physisch zu vernichten. Elektronische Informationen müssen mit einer geeigneten Löschungssoftware bearbeitet werden. Lediglich eine Einschränkung des Zugriffs auf die Informationen erfüllt diese Bestimmung nicht. Ebenfalls zu vernichten sind allfällige Doppel jener Informationen, die vom zuständigen Archiv übernommen wurden. Nach der Archivierung der Dossiers dürfen folglich nur noch im zuständigen Archiv Informationen zu den entsprechenden Geschäftsfällen vorhanden sein.* *Abs. 4 entspricht § 10 Abs. 4 Archivverordnung.*
Rechte des Archivs	§ 10. Das zuständige Archiv a. hat Zugang zu den Dossiers der öffentlichen Organe, soweit es zur Erfüllung seiner Aufgaben notwendig ist, b. kann für die Anbietung und die Übernahme von Informationen Weisungen erlassen, c. wird bei Projekten zur elektronischen Informationsverwaltung angehört.	*Die vorliegenden Regelungen werden von §§ 15 und 16 Archivverordnung hierher überführt, weil sie grösstenteils bereits vor der Übernahme der Informationen ins Archiv in die Informations-verwaltung der öffentlichen Organe eingreifen.*

	E. Informationssicherheit	
Zuständigkeit	§ 11. Das öffentliche Organ legt in seinem Zuständigkeitsbereich angemessene Massnahmen zum Schutz von Informationen gemäss den gesetzlichen Vorgaben, insbesondere gemäss § 7 IDG, fest.	*Das öffentliche Organ ist in seinem Zuständigkeitsbereich für die Einhaltung und Umsetzung der im IDG verankerten Grundsätze im Umgang mit Informationen verantwortlich. Dazu legt es die Aufgaben, Kompetenzen und Verantwortlichkeiten im Bereich Informationssicherheit fest.* *Das öffentliche Organ regelt selbständig, wie es die Informationssicherheit verwirklichen will. Es bleibt jedoch – unabhängig von einer allfälligen Übertragung der Aufgabe an Verwaltungseinheiten, Ämter oder externe Dritte – immer dafür verantwortlich.* *In einem ersten Schritt ermittelt das öffentliche Organ die für seine Informationen vorgegebenen Schutzziele. Allgemein gültig sind nach § 7 Abs. 2 lit. a–e IDG die folgenden Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachvollziehbarkeit. Darüber hinaus können für bestimmte Informationen spezielle rechtliche Vorgaben gelten (vgl. dazu beispielsweise das Personalgesetz, das Gesetz über die Auslagerung von Informatikdienstleistungen oder das Archivgesetz).* *Zur Erreichung der Schutzziele legt das öffentliche Organ geeignete Massnahmen fest, wobei gemäss § 7 Abs. 3 IDG die Art (Schutzwürdigkeit) der Information, die Art und der Zweck der Verwendung sowie der jeweilige Stand der Technik zu berücksichtigen sind. Die Massnahmen orientieren sich an allgemein anerkannten internationalen Standards. Aktuell ist ein Management der*

		Informationssicherheit nach den Normen der ISO-27000-Reihe anzustreben. Insbesondere ist sicherzustellen, dass das Thema als ständiger Prozess wahrgenommen und das Sicherheits-bewusstsein der Mitarbeitenden regelmässig geschult wird. *Sicherheitsmassnahmen sind organisatorischer oder technischer Natur. Diese müssen immer in einem angemessenen wirtschaftlichen Verhältnis zum möglichen Schaden stehen.* *Im Rahmen von Projekten und Systeman-passungen hat das öffentliche Organ frühzeitig die Anforderungen an die Informationssicherheit festzulegen und zu berücksichtigen. Die dafür nötigen Aufwendungen sind Teil der Projekt- und Betriebskosten und entsprechend zu budgetieren.*
Massnahmen	§ 12. Massnahmen zum Schutz von Informationen sind insbesondere: a. Berechtigungs- und Zugriffskonzepte, b. Verschlüsselung und Anonymisierung von Personendaten, c. Verwendung digitaler Zertifikate, d. Aufbau von Redundanzen, e. Zutrittskonzepte und Zutrittskontrollsysteme, f. Protokollierung von Zugriffen und Änderungen, g. Verwendung alterungsbeständiger Informationsträger, h. sichere Aufbewahrung physischer Informationsträger (insbesondere Schutz vor Feuchtigkeit und Feuer), i. Vorsorgemassnahmen für Notfälle und Krisenlagen.	*Die Informationssicherheit erstreckt sich auf alle Arten von Informationsträgern (Papier, Tonbänder, Filme, elektronische Datenträger).* *Neben den üblichen Massnahmen regelt das öffentliche Organ mit entsprechenden Konzepten, wie die Informationssicherheit bei Notfällen und in Krisenlagen sicherzustellen ist, z. B. wie bei einem Ausfall von Informatik-Systemen vorzugehen ist, der länger als die definierten Verfügbarkeits-anforderungen dauert.*
Überprüfung	§ 13. Das öffentliche Organ überprüft die Massnahmen	*Das öffentliche Organ überprüft mindestens alle*

	regelmässig und passt sie an, wenn die Schutzziele gemäss § 7 Abs. 2 IDG nicht mehr erreicht werden. Die Resultate der Überprüfung und die Anpassung der Massnahmen werden dokumentiert.	*zwei Jahre, ob die Sicherheitsmassnahmen angemessen sind und ob sie umgesetzt werden.*
Informations-bearbeitung durch Dritte	§ 14. Beauftragt das öffentliche Organ Dritte mit der Informationsbearbeitung, verpflichtet es diese zur Umsetzung der festgelegten Massnahmen zum Schutz von Informationen. Es überprüft die Umsetzung der Massnahmen regelmässig.	*Die Regelungen betreffend die Bearbeitung von Informationen durch externe Dritte gemäss § 6 IDG sowie § 25 IDV gelten auch für die Informations-sicherheit. Das heisst insbesondere, dass die Verantwortung für die Sicherheit der Informationen beim zuständigen öffentlichen Organ verbleibt.*