

zur Verordnung über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (VVS-ÜPF; SR ...)**1. Ausgangslage**

Der Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) des Eidgenössischen Justiz- und Polizeidepartements hat insbesondere den Auftrag, die Überwachung des Post- und Fernmeldeverkehrs sicherzustellen, die technische Entwicklung in diesem Bereich zu verfolgen und die entsprechenden Anpassungen der rechtlichen Grundlagen anzustreben. Zur Erfüllung seiner Aufgaben betreibt der Dienst ÜPF ein Verarbeitungssystem (V-FMÜ) zur Bearbeitung der Auskünfte, zur Verarbeitung der Überwachungen des Fernmeldeverkehrs, zur Geschäfts- und Auftragsverwaltung, zur Aufbewahrung über einen längeren Zeitraum und für die Protokollierung. Die aufgrund der Revision des Bundesgesetzes vom 18. März 2016¹ betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) neu geschaffenen gesetzlichen Grundlagen erfordern zusätzliche Funktionen (wie Langzeitdatenaufbewahrung, Schulungsinfrastruktur). Zudem automatisiert das neue V-FMÜ möglichst viele Abläufe und garantiert damit eine hohe Durchgängigkeit bei der Verarbeitung der Auskunfts- und Überwachungsdaten ohne Medienbrüche.

Um die Verordnung vom xx.xx.xxxx² über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) aus Gründen der Lesbarkeit zu entlasten und dem Gebot der Transparenz nachzukommen, werden die rechtlichen Grundlagen für das V-FMÜ, neben denjenigen in der BÜPF, in einer neuen Verordnung verankert.

2. Erläuterungen zu den einzelnen Bestimmungen*Ingress*

Die VVS-ÜPF stützt sich auf die Artikel 10 Absatz 4, 11 Absatz 6 und 12 Absatz 2 BÜPF. Sie konkretisiert insgesamt die Artikel 6-14 BÜPF, die Bestimmungen zum vom Dienst ÜPF zu betreibenden Informatiksystem enthalten und in der Botschaft³ entsprechend ausgeführt werden.

1. Abschnitt: Allgemeine Bestimmungen*Art. 1* Gegenstand

Diese Verordnung regelt, wie das V-FMÜ des Dienstes ÜPF für die Überwachung des Post- und Fernmeldeverkehrs betrieben und benutzt wird.

1 SR 780.1

2 SR 780.11

3 BBl 2013 2711-2721

Der Zweck des V-FMÜ wird für den Fernmeldeverkehr bereits in Artikel 7 BÜPF geregelt.

Art. 2 Datenausleitungsnetzwerk

Nach *Absatz 1* werden die durch die Fernmeldediensteanbieterinnen (FDA), ausgenommen die FDA mit reduzierten Überwachungspflichten gemäss Artikel 49 Absatz 1 VÜPF, und Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten gemäss Artikel 21 Absatz 1 VÜPF oder mit weitergehenden Überwachungspflichten gemäss Artikel 50 Absatz 1 VÜPF zu liefernden Daten (Auskünfte und Überwachungen) über ein Datenausleitungsnetzwerk (wie Glasfaser, VPN) direkt von den Mitwirkungspflichtigen bis zur Schnittstelle des Dienstes ÜPF ausgeleitet; die technischen Details, wie Übergabepunkte sind im Anhang der Verordnung vom xx.xx.xxxx⁴ des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) geregelt (vgl. Art. 12 Abs. 3 BÜPF). Die genannten Anbieterinnen betreiben dieses Datenausleitungsnetzwerk und haben die anfallenden Kosten für die Übermittlung der Daten gemäss Artikel 38 Absatz 1 BÜPF bis zur Übergabeschnittstelle an den Dienst ÜPF zu tragen. Die Datenlieferung stellt einen Teil der Überwachungsbereitschaft dar und ist dementsprechend von den Mitwirkungspflichtigen als Bringschuld zu tragen. Ebenso führt Artikel 51 Absatz 2 VÜPF aus, dass die Mitwirkungspflichtigen bestehende Netzzugänge zu öffentlichen Fernmeldenetzen kostenlos zur Verfügung stellen beziehungsweise diese in Absprache mit dem Dienst ÜPF oder dessen Beauftragten, soweit dies für die Überwachung notwendig ist, erstellen.

Nach *Absatz 2* kann auch die Kommunikation zwischen den Mitwirkungspflichtigen und dem Dienst ÜPF über dieses gesicherte Netzwerk erfolgen. So kann bei Unklarheiten, Fragen oder Problemen zu Anfragen oder Anordnungen über dieses Netzwerk kommuniziert werden.

Absatz 3 überträgt dem EJPD die Aufgabe, Detailbestimmungen zu erlassen und darin die technischen und administrativen Bestimmungen zu regeln, wie zum Aufbau, der Funktionsweise und dem Betrieb des Datenausleitungsnetzwerks.

2. Abschnitt: Daten und Datenbearbeitung

Art. 3 Daten

Der Inhalt des V-FMÜ wird in Artikel 8 BÜPF aufgeführt. *Absatz 1* beschreibt wie die verschiedenen Daten gewonnen werden; unabhängig davon, ob diese nun über eine längere Zeit aufbewahrt werden oder nicht. Artikel 8 BÜPF führt insbesondere diejenigen Daten auf, die im Rahmen einer Überwachung des Fernmeldeverkehrs beschafft werden dürfen. Vorliegender Artikel führt die Daten auf, die im V-FMÜ enthalten sind. Dazu gehören Personendaten wie auch reine Sachdaten. Ebenso die Daten, die von den Behörden selbst angefügt wurden, sei dies zur

⁴ SR XXX

einfacheren Darstellung mittels spezieller Programme oder als Bearbeitungsmerkmale wie das manuelle Einfügen von Kommentaren oder Informationen zu Adressierungselementen.

Bei den in *Buchstabe a* genannten Daten aus den Auskünften und Überwachungen handelt es sich um die von den Mitwirkungspflichtigen an das V-FMÜ gelieferten unbearbeiteten Daten, dazu gehören auch die Angaben über Fernmeldedienste (Art. 8 Bst. c BÜPF). Diese sind in den in der VD-ÜPF festgelegten Formaten auszuleiten. Damit diese Daten von den auswertenden Behörden einfacher ausgewertet werden können, werden sie aufbereitet. Die Daten werden dabei vereinheitlicht (wie einheitliche Zeitformate), les-, hör- und sichtbar gemacht (wie Darstellung auf Karten, Zuordnung der Nummern zu lesbaren Namen) und Duplikate und Fehler soweit möglich entfernt (*Bst. b*). Diese Daten können mittels Abrufverfahren (Online-Zugriff) bearbeitet werden.

Die auswertenden Behörden benötigen die Möglichkeit, Bearbeitungsmerkmale wie Markierungen, Hervorhebungen, Verschriftungen zu gewissen Daten anfügen zu können (*Bst. c*).

Die in *Buchstabe d* genannten Daten werden vom Dienst ÜPF zur Erledigung seiner Aufgaben benötigt, wie Auftragsverwaltungsdaten, Verfügungen, Genehmigungen, Zugriffsberechtigungen und auch Daten betreffend die Kontrollen (wie Qualitätsmanagement) und Statistiken des Dienstes ÜPF. Auch bearbeitet er zur Rechnungsstellung gemäss Artikel 38 BÜPF Buchhaltungsdaten, damit er die in der Verordnung vom xx.xx.xxxx über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF) festgelegten Gebühren erheben und die entsprechenden Entschädigungen auszahlen kann. Das Qualitätsmanagement wird in Artikel 18 BÜPF und Artikel 27 VÜPF respektive in der VD-ÜPF und dessen Anhang geregelt und in der Botschaft zum BÜPF⁵ (nachfolgend Botschaft genannt) vom 27. Februar 2013 (S. 2729) respektive in den entsprechenden erläuternden Berichten ausgeführt. Die Statistiken des Dienstes ÜPF zu den Überwachungen werden in den Artikeln 16 Buchstabe k, 35 Absatz 3 und 36 Absatz 2 BÜPF und im Artikel 12 VÜPF geregelt. Nach gängiger Praxis erstellt der Dienst ÜPF aber auch eine Statistik zu den Auskünften. Dies wird er auch unter dem neuen Recht weiterführen. Die Statistiken der Staatsanwaltschaften und der militärischen Untersuchungsrichter werden durch den Dienstes ÜPF veröffentlicht und werden in den Artikel 269^{bis} Absatz 2 und 269^{ter} Absatz 4 StPO, den Artikel 70^{bis} Absatz 2 und 70^{ter} Absatz 4 Militärstrafprozess vom 23. März 1979⁶ und Artikel 13 VÜPF geregelt. Diese Artikel der BÜPF wurden erst in der parlamentarischen Beratung aufgenommen und sind deshalb in der Botschaft noch nicht erläutert. Entsprechende Erläuterungen sind jedoch im erläuternden Bericht zu Artikel 27 VÜPF zu finden.

Nach *Buchstabe e* dürfen zusätzliche Daten genutzt werden um die Daten aus Auskünften und Überwachungen einfacher verständlich darzustellen. Es handelt sich beispielsweise um Karteninformationen oder Daten aus Nummernportierungs-

⁵ BBl 2013 2683 ff.
⁶ SR 322.1

datenbanken. Die Darstellung ist weit zu verstehen, so kann eine Darstellung auf Karten möglich sein, die Dekodierung oder der Vergleich mit anderen Daten.

Das V-FMÜ enthält nach *Buchstaben f* auch kryptografische Schlüssel. Damit können die mit dem öffentlichen Schlüssel des Empfängers verschlüsselten empfangenen Nachrichten mit dem privaten Schlüssel entschlüsselt werden. Es können Nachrichten mit einem öffentlichen Schlüssel des Empfängers verschlüsselt und mit dem privaten Schlüssel signiert werden. Zudem kann der Empfänger die Echtheit der empfangenen Nachricht mit dem öffentlichen Schlüssel des Absenders (Signatur) überprüfen.

Hilfsdateien wie Daten aus der Protokollierung oder Filterung werden in diesem Artikel nicht speziell aufgeführt, werden allerdings auch im V-FMÜ bearbeitet. Der Inhalt des V-FMÜ wird in Artikel 8 BÜPF aufgeführt.

Das V-FMÜ ermöglicht dem Dienst ÜPF die Bearbeitung der Daten, die er zur Erfüllung seiner Aufgaben benötigt. In *Absatz 2* wird dargestellt, wie dieses aufgebaut ist. Das V-FMÜ ist ein System, das die anfallenden Daten zentral bearbeitet, da ein übergreifendes Bearbeiten bei den verschiedenen Daten (wie Auskünfte, Historische Daten, Echtzeit, Kommentierungen und Übersetzungen, unabhängig ob in einem Strafverfahren, zur Notsuche oder Fahndung) hilfreich ist. Zudem können keine dedizierten Subsysteme des V-FMÜ ausgeschieden werden, weil es sich beim V-FMÜ um eine logische Einheit handelt.

Nach *Buchstabe a* umfasst das V-FMÜ die Aufgaben des heutigen „Call Center Information System“ (CCIS) sowie die zusätzlichen Aufgaben, die das BÜPF vorsieht. Dies beinhaltet vor allem die einfachen Auskünften zu Adressierungselementen sowie die technischen und administrativen Auskünfte zu Vertragsbestandteilen und der Netzinfrastruktur.

Nach *Buchstabe b* umfasst das V-FMÜ die Echtzeitdatenauswertung innerhalb des V-FMÜ. Hierzu zählt die Ausleitung der Inhalt- und Randdaten in Echtzeit, das heisst wie sie bei der Mitwirkungspflichtigen anfallen. Dabei werden die erhaltenen Daten durch entsprechende Bearbeitungsfunktionen für die auswertenden Behörden in einer verständlichen Form dargestellt. Das System stellt hierfür die entsprechenden Decoder und Analysefunktionen zur Verfügung.

Nach *Buchstabe c* umfasst das V-FMÜ Bearbeitungsmöglichkeiten für die historischen Daten (HD). Hierzu zählt die Ausleitung der Randdaten der bis sechs Monaten zurückliegenden Kommunikation. Auch hier sind die erhaltenen Daten durch entsprechende Bearbeitungsfunktionen für die auswertenden Behörden in einer verständlichen Form darzustellen. Das System stellt auch hierfür die entsprechenden Decoder und Analysefunktionen zur Verfügung.

Nach *Buchstabe d* kann der Dienst ÜPF mit dem V-FMÜ die von ihm benötigte Geschäftsabwicklung und -kontrolle durchführen. Es dokumentiert unter anderem die Tätigkeit des Dienstes ÜPF und verwaltet Unterlagen und Dossiers, so dass der Dienst ÜPF diese Daten bearbeiten kann. Darunter fallen auch die Daten zum Qualitätsmanagement, zur Statistik und die Rechnungsstellung mit den notwendigen Buchhaltungsdaten. Das V-FMÜ ist darauf auszurichten, dass es den Dienst ÜPF bei seinen Aufgaben betreffend die Qualität der von den Anbieterinnen gelie-

ferten Daten und die Statistik unterstützt. Die dabei zu bearbeitenden Daten sind in Artikel 6 aufgeführt.

Nach *Absatz 3* werden die Daten für die Aufbewahrung über eine längere Zeit im V-FMÜ aufbewahrt. Hierzu stellt das V-FMÜ entsprechende technische Lösungen bereit, welche je nach Datentyp oder Datenvolumen angepasst umgesetzt werden. Zudem ermöglicht das V-FMÜ die Protokollierung der Bearbeitung, auch das Ändern und Lesen von Daten gehört dazu, zum Beispiel mittels Logdateien. Die Protokollierung wird in Artikel 10 näher ausgeführt.

Art. 4 Herkunft der Daten

In *Artikel 4* wird ausgeführt, wer die Daten generieren darf respektive woher die Daten stammen.

Die Daten können von den Strafbehörden stammen, welche beispielsweise Kommentierungen oder Dokumentierungen über das Abrufverfahren (Online-Zugriff) anbringen (*Abs. 1 Bst. a*).

Sie können von den Mitwirkungspflichtigen stammen, welche die Daten dem Dienst ÜPF über das Datenausleitungsnetzwerk oder einem anderen durch den Dienst ÜPF zugelassenen Mittel übertragen (*Bst. b*).

Auch der Dienst ÜPF generiert Daten, seien dies Journale, Vermerke der Mitarbeitenden oder Protokollierungen (*Bst. c*).

Daten sollen aber auch von Datenbanken – unabhängig, ob öffentlich zugänglich Quellen oder nicht – importiert werden können (*Bst. d*), wie der Nummernportierungsdatenbank "Telecom Data Service" (TelDas) oder für IP-Adressbereichsabfragen beim "Réseaux IP Européens" (RIPE).

Ebenso sollen Geoinformationen und Kartenmaterial genutzt werden können, um Koordinaten einfacher darzustellen (*Bst. e*). Bei Notsuchen können die Personen auf diese Weise einfacher lokalisiert werden. Weiter können Bewegungs- und Aufenthaltsprofile erstellt werden, die beispielsweise durch das Kartenmaterial von Swisstopo (Geologie, Gebäude und Anlagen), ergänzt werden können. Der Abruf des Materials und der Informationen ist so durchzuführen, dass keine Hinweise auf laufende Abklärungen an die Serviceanbieter und Hosting Provider übermittelt werden, da sich diese auf Servern von ausländischen Anbietern im Ausland befinden können.

Absatz 2 führt aus, dass von den auswertenden Behörden (*Art. 4 Abs. 1 Bst. a*) lediglich die in Artikel 3 Absatz 1 Buchstabe c aufgeführten Bearbeitungsmerkmale und die in Buchstabe f genannten kryptografischen Schlüssel ergänzt werden dürfen. Der Import von kryptografischen Schlüsseln ist unverzichtbar, um verschlüsselte Überwachungsdaten überhaupt darstellen und bearbeiten zu können (vgl. *Art. 7 BÜPF*, insb. *Bst. a, b und d*). Ein weitergehender Import von Ermittlungsdaten ist klar ausgeschlossen.

Art. 5 Bearbeitungsfunktionen für Daten aus Auskünften und Überwachungen

Artikel 5 und 6 regeln wichtige Grundsätze der Bearbeitung von Daten im V-FMÜ. Da in diesem auch besonders schützenswerte Personendaten bearbeitet werden, braucht es dazu eine formell gesetzliche Grundlage, die sich grundsätzlich aus den Artikeln des 2. Abschnitts des BÜPF ergibt. Besonders schützenswerte Personendaten werden vor allem im Rahmen von Überwachungen, allerdings nicht im Rahmen von Auskünften, bearbeitet. Unter besonders schützenswerten Personendaten versteht man Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen (vgl. Art. 3 des Bundesgesetzes vom 19. Juni 1992⁷ über den Datenschutz [DSG]). Die Definition ist abschliessend.

Artikel 5 führt nun auf Verordnungsstufe die Bearbeitungsfunktionen für Auskünfte und Überwachungen gemäss Artikel 7 Buchstabe d BÜPF auf. Demnach dient das V-FMÜ dazu, Bearbeitungsfunktionen für die im System gespeicherten Daten anzubieten. Die Botschaft hält dazu fest, dass die Auswertung der Überwachungsdaten durch die Strafverfolgungsbehörden in den entsprechenden Informationssystemen des polizeilichen Informationssystem-Verbundes des Bundesamtes für Polizei erfolgt (vgl. Botschaft, BBl 2013 2683, 2714).

Im Rahmen der Arbeiten der Ordnungsrevisionen stellte sich die Abgrenzungproblematik zwischen den Bearbeitungsfunktionen nach Artikel 7 Buchstabe d BÜPF und der Datenbearbeitung nach dem Bundesgesetz vom 13. Juni 2008⁸ über die polizeilichen Informationssysteme des Bundes (BPI). Dieselbe Problematik stellt sich auch in Bezug auf die Datenbearbeitung zum Informationssystem des Nachrichtendienstes. Konkret stellt sich die Frage, ob Analysefunktionen, vor allem diejenigen, die einen Mehrwert für die Ermittlungen erbringen, im Rahmen der Bearbeitungsfunktionen des V-FMÜ genutzt werden dürfen. Selbstverständlich werden dabei keine nicht öffentlichen Personendaten aus Quellen ausserhalb der Fernmeldeüberwachung importiert. Eine ausdrückliche gesetzliche Grundlage für diese Funktionen ist im BÜPF nicht vorhanden. Trotzdem sollen solche Funktionen im V-FMÜ weiterbetrieben beziehungsweise neu implementiert werden können, dies in Anwendung der Figur der progressiven Sanierung der Rechtslage und weil die umstrittenen Funktionen zum Standardfunktionsumfang des vom Dienst ÜPF beschafften Fernmeldeüberwachungssystems gehören und gleichzeitig die bei fedpol und beim NDB vorhandenen Systemen über keine vergleichbaren Funktionen verfügen. Ansonsten wäre mit hohen Kosten zu rechnen, wenn in den Systemen nach BPI und NDG dieselben Funktionen neu implementiert werden müssten, die im V-FMÜ bereits enthalten sind. Mit der bereits geplanten Revision des BPI ist eine Klärung der Abgrenzung der verschiedenen Systeme anzustreben und klare gesetzliche Grundlagen zu schaffen, wobei die rasante Weiterentwicklung und die Innovationen der informations- und kommunikationstechnologischen (IKT-)Mittel

7 SR 235.1
8 SR 361

einerseits nicht behindert und diese andererseits nicht hoffnungslos hinterhergehinkt werden soll.

In Artikel 5 werden die Bearbeitungsfunktionen des V-FMÜ, auch solche, die einen Mehrwert für die Ermittlungen ermöglichen, abschliessend im Detail aufgeführt. Somit können sämtliche von den Mitwirkungspflichtigen ins V-FMÜ gelieferten Daten von den zugriffsberechtigten Behörden bearbeitet werden. Artikel 9 Absatz 1 und 2 BÜPF bezeichnet wer als zugriffsberechtigte Behörde gilt und somit die Daten bearbeiten darf. Im V-FMÜ können die von den Mitwirkungspflichtigen gelieferten Daten mit weiteren Daten (s. d. Art. 4 Herkunft der Daten) ergänzt werden. Allerdings dürfen keine schützenswerte Personendaten aus weiteren Quellen ausserhalb der Fernmeldeüberwachung, das heisst auch keine Daten aus Überwachungen mit IMSI-Catchern und GovWare nach den neuen Artikeln 269^{bis}–269^{quater} StPO oder Artikeln 70^{bis}–70^{quater} MStP, im V-FMÜ genutzt werden, wenn diese nicht unabdingbar zur Darstellung der bereits gewonnenen Daten benötigt werden, wie kryptografische Schlüssel. Das V-FMÜ kann zudem Korrespondenzdaten versenden und entgegennehmen, wie E-Mails, Fax, SMS, Telefonanrufe.

Nach *Buchstaben a* können einerseits vor allem Überwachungen in Echtzeit mitgehört werden, wie über Telefonie mit oder ohne Bild oder über VoIP. Andererseits können aufgezeichnete Gespräche zeitverzögert abgespielt (Nachhören) werden.

Nach *Buchstaben b* können die gewonnenen Daten angezeigt und gedruckt werden. Dazu gehört vor allem die Protokollanalyse, aber auch Statusanzeigen, wie ob ein Telefon ein- oder ausgeschaltet wurde. Die Daten, wie SMS, E-Mail oder http-Informationen, aber auch Gespräche, werden so aufbereitet, dass sie möglichst verständlich angezeigt werden und so einfach durch die Strafverfolgungsbehörden ausgewertet werden können. Bei den von den Mitwirkungspflichtigen erhaltenen Daten, gerade bei einer Überwachung eines Internetanschlusses, handelt es sich um eine Abfolge von Zahlen und Buchstaben in grosser Menge. Diese werden mit verschiedenen Instrumenten beispielsweise so dargestellt, dass Bilder, die während einer Internetsitzung heruntergeladen wurden, wieder als solche erkennbar sind. Gedruckt werden vor allem Fallinformationen, die beispielweise für die Staatsanwaltschaft ausgedruckt werden.

Nach *Buchstabe c* können die erhaltenen Daten über die Mobilfunktelefone dank den bei einer Massnahme erhaltenen Koordinaten lokalisiert werden. Zum einfacheren Bearbeiten können diese in einer geografischen Karte mit weiteren Daten dargestellt werden, so dass beispielsweise bei einer Notsuche der Standort der vermissten Person schneller gefunden werden kann.

Durch das Dekodieren nach *Buchstabe d* werden die Daten in andere Formate umgewandelt. Beispielsweise werden empfangene oder gesendete Daten oft in spezielle Formate umgewandelt, um sie für die Übertragung zu komprimieren. Anschliessend sind sie wieder in die ursprünglichen Formate zu überführen. Die Daten werden allerdings nicht nur kodiert, sondern auch zum Schutz vor ungewolltem Lesen verschlüsselt. Mit dem entsprechenden Schlüssel können diese wieder leserlich gemacht werden.

Nach *Buchstabe e* können die verschiedenen Elemente gruppiert und sortiert werden. Dies ermöglicht eine bessere Übersicht und führt dazu, dass die einzelnen Elemente besser verglichen werden können.

Nach *Buchstabe f* ist auch die Suche beispielsweise nach einem bestimmten Text oder das Filtern wie nach einem bestimmten Meldungstyp (z. B. E-Mail, SMS, Gespräch, Stichworten, Zeitabschnitten, geografischen Gebieten) möglich. Diese Filterung ist nicht mit der vorgängig durch den Dienst ÜPF vorzunehmenden automatischen Filterung nach Artikel 7 VÜPF respektive Artikel 17 Buchstabe g BÜPF zu verwechseln. Bei letzterer werden die Daten im V-FMÜ nicht gespeichert, bei ersterer kann die Filterung wieder rückgängig gemacht werden, so dass wieder sämtliche Daten angezeigt werden.

Mit der Bearbeitungsfunktion nach *Buchstabe g* kann das System eine Stimme anhand einer vorhandenen Sprachaufnahme einer bestimmten Person zuordnen. Beispielsweise kann so einfacher festgestellt werden, mit wem ein Gespräch geführt wird.

Nach *Buchstabe h* können Ton- und Filmdokumente verschriftet werden, das heisst das Gesprochene und Gesehene wird in Protokollform festgehalten und nötigenfalls in eine Landessprache übersetzt. Bei der Fernmeldeüberwachung steht die Niederschrift des gesprochenen Wortes grundsätzlich im Vordergrund.

Nach *Buchstabe i* können die entsprechenden Elemente kommentiert werden, wie mit Stichworten über Eindrücke und Erkenntnisse oder über Fallnamen.

Mit der Alarmierung nach *Buchstabe j* informiert das System beispielsweise per Telefon oder SMS, dass ein bestimmtes Ereignis eingetreten ist.

Nach *Buchstabe k* können benötigte Informationen vor allem an dazu berechtigten Personen der Strafverfolgungsbehörden gesichert übermittelt werden. Auf diese Weise können Ermittler benötigte Daten herunterladen.

Nach *Buchstabe l* können Informationen vom Dienst ÜPF vernichtet werden. Diese Ausnahmefunktion kommt allerdings nur bei der Triage nach Artikel 16 Buchstabe e BÜPF auf Anweisung des zuständigen Gerichts zur Anwendung.

Nach *Absatz 2* sollen die Funktionen nur diejenigen Daten umfassen, auf welche die bearbeitenden Personen Zugriff haben. So dürfen beispielsweise bei einer Suche oder einem Filtern von Daten nur diejenigen Daten erscheinen, auf welche die Person berechtigt ist.

Art. 6 Datenbearbeitung für die Geschäftsabwicklung und -kontrolle

Der Dienst ÜPF arbeitet nur auf Anordnung, hauptsächlich auf Anordnung der Strafverfolgungsbehörden, da er keine Strafverfolgungskompetenz hat. Er ist grundsätzlich nur Betreiber (Art. 6 BÜPF) des V-FMÜ, aber nicht Datenherr (Art. 13 BÜPF). Die anordnenden Behörden sind die Inhaberinnen der Daten, die der Dienst ÜPF in Erfüllung seiner Aufgaben einfordert, entgegennimmt und gemäss der Zugriffsberechtigung für den Online-Zugriff bereitstellt. Der Dienst ÜPF ist jedoch Inhaber der Daten, die er zur Geschäftsabwicklung und -kontrolle (Art. 3 Abs. 2 Bst. d) sowie aus der Protokollierung generiert.

Die vom Dienst ÜPF für die Ausführung der Anordnungen zur Überwachung des Fernmeldeverkehrs und die Kontrolle dieser Ausführung bearbeiteten Daten werden in diesem Artikel aufgeführt.

Der Dienst ÜPF erteilt gestützt auf die in *Buchstabe a* aufgeführten Kontaktdaten den von der Behörde bezeichneten Personen der bezeichneten Behörde, meist der ermittelnden Polizeibehörde, die Zugriffsrechte im V-FMÜ, nimmt bei Unklarheiten mit diesen Rücksprache und stellt den anordnenden Behörden die Rechnung zu. Diese Daten können bereits vor einer ersten Anordnung im System gespeichert werden. Bei der Anordnung einer Überwachung sind die Daten dann bereits im System vorhanden und müssen nicht vorgängig erfasst werden. Zudem können die erfassten Behörden über Neuerungen informiert werden.

Die Angaben nach *Buchstabe b* dienen den Mitwirkungspflichtigen und dem Dienst ÜPF zur Kontrolle, ob die zu überwachende Anwendung beziehungsweise der zu überwachende Internetzugang mit dieser Person in Zusammenhang stehen. Zudem kann der Dienst ÜPF anhand der Berufsbezeichnung überprüfen, ob die notwendigen Vorkehren gemäss Artikel 271 Absatz 1 StPO getroffen wurden (Art. 5 VÜPF).

Der Dienst ÜPF prüft gestützt auf die Angaben von *Buchstabe c* formell, ob diese Straftat beziehungsweise Straftaten die Anordnung dieser Überwachung nach dem Katalog in Artikel 269 StPO oder nach Artikel 273 StPO (rückwirkende Überwachungen) erlaubt beziehungsweise erlauben. Zudem benötigt er diese Angaben, um jährlich eine Statistik zu den Überwachungsaufträgen und Auskünften des Post- und Fernmeldeverkehrs zu erstellen.

Unter *Buchstabe d* sind die angeordneten Auskunfts- und Überwachungstypen aufgeführt. Diese werden den Mitwirkungspflichtigen in Auftrag gegeben, fakturiert und für die Statistik ausgewertet.

Nach *Buchstabe e* können sämtliche Korrespondenz, allfällige Gesprächsnotizen, aber auch mündliche Mitteilungen sowie die zu Beweiszwecken aufgezeichneten Telefonate nach Artikel 8 VÜPF, die bei der Geschäftsabwicklung und -kontrolle entstehen, im V-FMÜ bearbeitet werden. Darunter fallen beispielsweise per Mail übertragene Sprachmitteilungen.

Nach *Buchstabe f* werden im V-FMÜ ebenfalls behördliche Verfügungen aufbewahrt. Dies können zu Beweiszwecken einerseits Verfügungen der Staatsanwaltschaften und Zwangsmassnahmengerichte (Anordnungen, Genehmigungen und Verlängerungen) sein. Andererseits gehören dazu auch die Verfügungen des Dienstes ÜPF (z. B. nach Art. 40 Abs. 1 BÜPF) sowie Beschwerdeentscheide der Gerichtsbehörden. So sollen möglichst alle Daten zu einem Dossier zentral gespeichert werden können. Die Daten, welche bei der Erarbeitung von Entscheiden des Dienstes ÜPF anfallen, werden im GEVER-System bearbeitet. Nur der Entscheid wird, wo sinnvoll, bei dem entsprechenden Dossier im V-FMÜ abgelegt.

Buchstabe g verweist auf die Artikel 15 Buchstaben h-k und 47 Absatz 1 Buchstaben h-l der VÜPF. Diese Buchstaben umfassen bestimmte Daten, die in den Überwachungsanordnungen aufzuführen sind. Weitere Hinweise können dem erläuternden Bericht der VÜPF zu den entsprechenden Bestimmungen entnommen werden.

Nach *Buchstaben h* können auch die durch die Staatsanwaltschaften vergebene Referenznummer und der Fallname, wie auch die eindeutige Referenznummer (LLID), die der Dienst ÜPF für jedes Dossier erstellt, aufgenommen werden.

Der Dienst ÜPF bearbeitet nach *Buchstabe i* die Kontaktdaten der Mitwirkungspflichtigen. Einerseits kann er gestützt auf diese Daten die Auskünfte und Überwachungen an die zuständige Mitwirkungspflichtige respektive deren Mitarbeitenden anordnen. Andererseits werden diese Informationen auch anderweitig benötigt, wie für die Prüfung und Bestätigung der Auskunfts- und Überwachungsbereitschaft.

Der Dienst ÜPF bearbeitet nach *Buchstabe j* ebenfalls weitere Daten der Mitwirkungspflichtigen, die er unter anderem für die Übermittlung der von den Mitwirkungspflichtigen übermittelten Daten, für die Prüfung der Auskunfts- und Überwachungsbereitschaft benötigt. Dies können Daten sein wie Zertifikate, Kennungen (Anbieter-, Unternehmens-Identifikationsnummer [Art. 38 Bst. a HRegV]⁹), Telefonnummern, IP-Adressen, Status der Auskunfts- und Überwachungsbereitschaft, Informationen zu den angebotenen Dienstleistungen, Informationen zu der geringen wirtschaftlichen Bedeutung nach Artikel 49 Absatz 1 VÜPF oder Informationen zu administrativen oder strafrechtlichen Sanktionen nach dem 10. und 11. Abschnitt des BÜPF.

Adressierungselemente dienen zum Aufbau der Kommunikation und können einer Person zugeordnet werden. Artikel 3 des Fernmeldegesetzes vom 30. April 1997¹⁰ (FMG) definiert sie als Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern. Sie sind in den meisten Anordnungen enthalten und sollen nach *Buchstabe k* auch im V-FMÜ bearbeitet werden. Ebenso können Identifikatoren bearbeitet werden, die im Gegensatz zu den Adressierungselementen einer Person nicht eindeutig zugeordnet werden können.

Nach *Buchstabe l* werden etliche weitere Informationen technischer Natur, die für die Ausführung der Anordnungen zur Überwachung des Fernmeldeverkehrs, inklusive Daten für die Spezialfälle, und die Kontrolle dieser Ausführung benötigt werden, im V-FMÜ gespeichert. Unter anderem sind dies die Schlüssel für die gesicherte Datenübertragung, die Portnummern oder Angaben für das Datenausleitungsnetzwerk (Art. 2) wie IP-Adressen und Passwörter.

Nach *Buchstabe m* werden im V-FMÜ auch Daten bearbeitet, damit einerseits die Gebühren von den Strafverfolgungsbehörden erhoben und andererseits die Entschädigungen an die Mitwirkungspflichtigen entrichtet werden können. Dazu gehört beispielsweise der Status der Abrechnung, die Gebühr für nicht aufgeführte Dienstleistungen, die nach Zeit- und Sachaufwand festgelegt wird (vgl. Art. 13 GebV-ÜPF).

⁹ SR 221.411; Handelsregisterverordnung vom 17.10.2007
¹⁰ SR 784.10

Art. 7 Zugriffsberechtigung auf das Verarbeitungssystem

Die Zugriffsrechte der verschiedenen Personen auf das V-FMÜ werden in Artikel 9 BÜPF allgemein geregelt. In Artikel 7 werden die grundsätzlichen Zugriffsberechtigungen zum System geregelt, in Artikel 8 die zusätzlichen Zugriffsberechtigungen auf die einzelnen Überwachungen.

Das V-FMÜ muss den Anforderungen verschiedenster Berechtigten, Behörden und Personen gerecht werden. Gleichzeitig muss es diverse Schnittstellen besitzen sowie Zugriffe durch Berechtigte oder Mitglieder der genannten Behörden (vgl. Art. 1 Abs. 2 Bst. a-f VÜPF) oder Berufsstände auf unterschiedliche Funktionen zulassen.

Nach *Absatz 1* wird der grundsätzliche Zugriff auf das V-FMÜ gewährt. Dieser wird benötigt um unter anderem Auskunftsgesuche und Überwachungsanordnungen einreichen zu können. Der Zugriff wird mit einem vom Dienst ÜPF zur Verfügung gestellten Formular beantragt. Die Einreichung beim Dienst ÜPF von vorzunehmenden Änderungen von Zugriffsrechten wird in Artikel 3 VÜPF geregelt. Alle erteilten Zugriffsberechtigungen werden einer natürlichen Person zugeteilt. Diese Person erhält ein eigenes Benutzerkonto und ist verantwortlich für die ausgeführten Zugriffe. Sie muss begründen können, weshalb sie zur Erfüllung ihrer Aufgaben auf die Daten zugreifen musste.

Zugriffsberechtigt sind nach *Buchstabe a* die Mitarbeitenden der berechtigten Behörden. Damit sind die Behörden gemeint, welche Überwachungen nach Artikel 9 BÜPF anordnen und Auskünfte nach Artikel 15 BÜPF beantragen können. Diese können im Rahmen eines Strafverfahrens, einer Notsuche oder Fahndung angefordert werden. Dies sind vor allem die Strafverfolgungsbehörden, wie fedpol, aber auch Behörden zwecks Erledigung von Verwaltungsstrafsachen. Auch kantonale Vollzugsbehörden können bei entsprechender kantonaler Rechtsgrundlage bei Fahndungen Überwachungen anordnen. Aber auch die kantonalen Strafbehörden, gegliedert in 26 Kantone, deren Zugriff auf die Überwachungsmassnahmen zur Ausübung von untersuchungsrichterlichen beziehungsweise gerichtlichen Aufgaben über einen gesicherten Zugang ins V-FMÜ erfolgt und auch die Polizeiorganisationen als auswertende Behörden, die über ein für den Zugriff autorisiertes Netzwerk auf die gespeicherten Daten zugreifen. Weiter benötigt auch die Bundesanwaltschaft als verfügende Strafverfolgungsbehörde des Bundes oder das Bundesstrafgericht einen Zugriff. Mit dem totalrevidierten Bundesgesetz vom 25. September 2015 über den Nachrichtendienst¹¹ erhält zudem auch der Nachrichtendienst die Möglichkeit, neben den Auskünften (Art. 25 Abs. 2 NDG) auch Überwachungen (Art. 26 Abs. 1 Bst. a NDG) anzuordnen.

[Artikel zum NDG nur, wenn dieses vor dem BÜPF oder gleichzeitig mit diesem in Kraft tritt.]

Zugriffsberechtigt sind nach *Buchstabe b* die Mitarbeitenden der FDA und der Anbieterinnen abgeleiteter Kommunikationsdienste, um Anfragen der anordnenden und auswertenden Behörden, die über das V-FMÜ an sie gelangen, via dieses V-FMÜ beantworten zu können. Die nur duldungspflichtigen Mitwirkungspflichtigen

¹¹ SR XX, Nachrichtendienstgesetz, NDG

werden in der Regel keinen Zugriff auf das V-FMÜ benötigen, da in diesen Fällen meist der Dienst ÜPF die anfallenden Aufgaben übernehmen wird.

Zugriffsberechtigt sind nach *Buchstabe c* die Mitarbeitenden des Dienstes ÜPF, um den Pflichten im Rahmen der Überwachung des Post- und Fernmeldeverkehrs nachkommen und die Wartung und den Support der Systeme sicherstellen zu können.

Schliesslich sind nach *Buchstabe d* Dritte zugriffsberechtigt, die vom Dienst ÜPF mit Wartungs-, Betriebs- und Programmieraufgaben betraut werden, wenn er diese Aufgaben nicht selbst wahrnehmen kann.

Nach *Absatz 2* sollen einzelne Mitarbeitende ("OrgAdmin") Zugriffe auch weiter vergeben können. Diese Zugriffe können allen Mitarbeitenden der entsprechenden Behörden erteilt werden. Die Berechtigung zur Weitervergabe der Zugriffe gibt der Dienst ÜPF auf Anordnung der zuständigen Person, beispielsweise des Polizeikommandanten. Dazu erhalten diese Mitarbeitenden spezielle Zugriffe (Nummertoken), die nur restriktiv weitergegeben werden sollen. So sollen Übersetzer, Gerichtsvertreter und Rechtsbeistände, wie Strafverteidigerinnen oder Strafverteidiger, zur Gewährung der gesetzlich verankerten Rechte Zugriff erhalten. Das Akteneinsichtsrecht wird durch die Inhaber der Datensammlung gewährt, welche nach Artikel 13 BÜPF die Behörden sind, die gemäss Artikel 9 BÜPF Zugriff auf das V-FMÜ haben. Diese Zugriffe erfolgen deshalb nicht vom individuellen PC des Rechtsbeistandes aus, sondern entweder mittels Abrufverfahren (Online-Zugriff) in von der Behörde, die mit dem Fall betraut ist, bestimmten Räumlichkeiten oder über eine andere Art, wie einen von der Behörde zur Verfügung gestellten Datenträger. Gerade bei Verfahren mit Zeugenschutz ist denkbar, dass die Behörde nur bestimmte Passagen einer Nachricht abspielen darf oder gewisse Protokolle schwärzen muss. Privatpersonen, die überwacht oder von der Überwachung mitbetroffen wurden und ihre Parteirechte geltend machen können, erhalten wie Rechtsbeistände einen Zugriff auf ihre Daten. Der Dienst ÜPF hat keinen direkten Kontakt zu den betroffenen Personen oder Rechtsbeiständen. Wenn ein solcher Nummer token an eine Drittperson weitergegeben wird, bleibt die nach Absatz 1 Buchstabe a zuständige Person (der Mitarbeiter der Behörde) verantwortlich, beispielsweise auch für den Verlust des Nummer token. Er hat die Benutzung des Nummer token detailliert zu dokumentieren damit für den Dienst ÜPF klar ersichtlich ist, wer, wann auf welche Daten Zugriff hatte.

Nach *Absatz 3* hat der Dienst ÜPF die Pflicht die Voraussetzungen für die Zugriffsberechtigungen periodisch zu prüfen. Damit soll unter anderem verhindert werden, dass aufgrund nicht gemeldeter Änderungen, wie Abgang oder Funktionswechsel eines Mitarbeiters, unnötige Zugriffe bestehen bleiben.

Nach *Absatz 4* sind die Zugriffsberechtigungen auf das V-FMÜ im Anhang zu regeln. Daraus ist ersichtlich, welchen Personengruppen auf welche Funktionen die Berechtigung erteilt werden darf. Genauer wird im Bearbeitungsreglement des Dienstes ÜPF festgehalten.

Art. 8 Zugriffsberechtigung auf Daten aus einzelnen Überwachungen

Wie heute kann eine Mitarbeiterin oder ein Mitarbeiter einer berechtigten Behörde, der Zugriff aufs V-FMÜ erhalten hat, die Applikation zum Bearbeiten der Überwachungsdaten starten. Die Daten werden allerdings noch nicht angezeigt. Nach *Absatz 1* muss er auf einzelne Überwachungsdaten berechtigt werden, um auf diese zugreifen zu können. Der Zugriff auf die einzelnen Überwachungen kann auf zwei verschiedene Weisen erfolgen. Einerseits erteilt der Dienst ÜPF den Zugriff an die Personen, welche in der Anordnung¹² aufgeführt sind. Andererseits kann ein nach Absatz 3 berechtigter Mitarbeitender der Behörde einen Zugriff an einen Mitarbeiter erteilen, sofern der diesen Zugriff zur Erfüllung seiner Aufgaben benötigt.

Nach *Absatz 2* können die in den Artikeln 279 StPO, 70j MStP, 33 NDG, 35 und 36 BÜPF, vor allem die überwachten beschuldigten und überwachten ehemals vermissten Personen, ein Gesuch bei der zuständigen Behörde einreichen, damit sie ihr Akteneinsichtsrecht beziehungsweise ihr Recht auf Auskunft über die Daten (vgl. Art. 10 Abs. 4 BÜPF) wahrnehmen können. Diese Rechte können aufgrund der jeweils anwendbaren Bestimmungen aufgeschoben oder eingeschränkt werden (bspw. Art. 279 Abs. 2 StPO, Art. 70j Abs. 2 MStP, Art. 63 Abs. 2, 4 und 5 NDG). Als zuständige Behörde gilt im Strafverfahren die mit dem Verfahren befasste Behörde, solange dieses noch nicht abgeschlossen ist. Anschliessend richtet sich das Auskunftsrecht nach dem Datenschutzgesetz des Bundes oder des jeweiligen Kantons (vgl. Art. 10 Abs. 1 Bst. b BÜPF), ebenso im Falle der Überwachung einer Notsuche oder Fahndung. Der Nachrichtendienst des Bundes (NDB) speichert die Daten aus genehmigungspflichtigen Beschaffungsmassnahmen, wie die Überwachungen des Post- und Fernmeldeverkehrs, fallbezogen und gesondert von den Informationssystemen nach Artikel 47 NDG (Art. 58 Abs. 1 NDG). Dort werden die Daten gesichtet. Nur für die Zwecke des Auftrags notwendigen Daten übernimmt der NDB zur weiteren Auswertung in die entsprechenden Informationssysteme des Verbunds. Das Auskunftsrecht im Falle einer vom NDB angeordneten Überwachung richtet sich nach Artikel 63 NDG. Danach prüft der NDB zuerst eine Auskunftserteilung, im Falle von Geheimhaltungsinteressen oder bei nicht verzeichneten Personen, kann er die Auskunft aufschieben. Die betroffene Person kann danach an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gelangen, der sinngemäss das frühere Verfahren der indirekten Auskunft durchführt. Der Dienst ÜPF nimmt keine solchen Gesuche entgegen, da er für deren Beurteilung nicht zuständig ist. Wird das Gesuch von der zuständigen Behörde gutgeheissen, erhalten die Personen entweder mittels Abrufverfahren (vorübergehenden Online-Zugriff beispielsweise via Nummerntoken) in von der Behörde bestimmten Räumlichkeiten oder über eine andere Art, wie einen von der Behörde zur Verfügung gestellten Datenträger, Zugriff auf die Daten. Sie sehen dabei die Überwachungsdaten, die für die Wahrnehmung ihrer Rechte notwendig sind. Mittels Abrufverfahren werden sie einzelne Visualisierungs- und Analysefunktionen des Verarbeitungssystems (wie das Drucken oder gesicherte Übermitteln an die berechtigten Personen) benutzen können, allerdings nur in dem Aus-

¹² vgl. Art. 3 VÜPF Einreichung der Anordnungen beim Dienst ÜPF

mass, wie sie es für die Wahrnehmung ihre Rechte benötigen. Bei Bedarf kann auch ein zusätzlicher Datenträger nach Artikel 9 GebV-ÜPF erstellt werden lassen. Ob sie den Zugriff unmittelbar selber oder ob sie ihn mit der Hilfe eines geschulten Polizisten vornehmen können, hängt vor allem von der entsprechenden Behörde ab. **[Artikel zum NDG nur, wenn dieses vor dem BÜPF oder gleichzeitig mit diesem in Kraft tritt.]**

Nach *Absatz 3* soll nicht nur der Dienst ÜPF Zugriffe auf Überwachungsdaten vergeben, sondern auch einzelne Mitarbeitende der Behörden sollen Zugriffe vergeben können. Dies macht Sinn, wenn besonders geschulte Mitarbeitende der Strafverfolgungsbehörde (sog. „OrgAdmin“) nach Anordnung der Überwachung weiteren Ermittlern aus ihrer Organisationseinheit Zugriff auf Überwachungsdaten eines bestimmten Falles gewähren oder entziehen sollen. Aber auch an Rechtsvertreter nach *Absatz 2* soll ein besonders geschulter Mitarbeitender ein Zugriff gewähren können. Da eine Mutation teilweise sehr rasch zu geschehen hat, ist es von Vorteil, wenn eine Person vor Ort diese vornehmen kann. Abgesehen davon, gibt der Dienst ÜPF nur auf Anweisung der anordnenden Behörde, wie der Strafverfolgungsbehörde, bestimmten Personen, wie den Polizeibeamten Zugriff auf Überwachungsdaten.

Nach *Absatz 4* sind auch zu diesen Zugriffsberechtigungen Regelungen in einem Bearbeitungsreglement vorzusehen.

Art. 9 Schnittstellen

Das V-FMÜ besitzt mehrere Schnittstellen, welche die notwendige gesetzliche Grundlage in Artikel 14 und 14a (Koordinationsbestimmung mit dem NDG) BÜPF haben.

Nach *Buchstabe a* besteht eine Schnittstelle zu den Systemen der Mitwirkungspflichtigen für die Übermittlung von Aufträgen, die Entgegennahme von Daten und Bestätigungen (Bestätigung des Erhalts des Auftrags vgl. Art. 9 Abs. 2 Bst. c VÜPF). Unter Aufträge fallen sowohl einfache, wie administrativ-technische Auskünfte und Überwachungen. Die entsprechenden technischen Vorschriften werden im Anhang 1 der VD-ÜPF ausgeführt.

Nach *Buchstabe b* können Daten zum polizeilichen Informationssystem-Verbund des Bundesamtes für Polizei und zum Informationssystem des Nachrichtendienstes kopiert werden. Das V-FMÜ erlaubt den Online-Zugriff inklusive das Kopieren von Daten und das Herunterladen der Daten mittels einer Schnittstelle zum polizeilichen Informationssystem-Verbund, konkret zur Ermittlerdatenbank (JANUS)¹³. Mit dem Inkrafttreten des später in Kraft tretenden Gesetzes, NDG oder BÜPF, wird eine zusätzliche Schnittstelle zum Informationssystem des Nachrichtendienstes in Artikel 14a BÜPF geschaffen. Somit können die Daten nach Artikel 9 Buchstabe b auch zum Informationssystem des Nachrichtendienstes kopiert werden. Das V-FMÜ erlaubt den Online-Zugriff inklusive das Kopieren von Daten und das Herunterladen der Daten mittels einer Schnittstelle zum Informationssystem des

¹⁴ Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001

Nachrichtendienstes. Das Kopieren in die Systeme der Kantone hat über eines dieser Systeme zu erfolgen.

Nach *Buchstabe c* können Schnittstellen auch für den Zugriff zu Datenbanken zur Abklärung von Adressierungselementen eingerichtet werden. Adressierungselementen in diesem Sinne können Kommunikationsparameter und Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern sein, aber auch Geoinformationen und Kartenmaterial. Diese Daten können beispielsweise von TelDas, RIPE oder swisstopo stammen. Dabei handelt es sich um reine Sachdaten, das heisst um Daten ohne Bezug zu bestimmten Personen.

3. Abschnitt: Datenschutz und Datensicherheit

Art. 10 Massnahmen für die Datensicherheit

Da das V-FMÜ besonders schützenswerte Personendaten enthält, sind umfassende Massnahmen, sowohl technischer wie organisatorischer Natur, zu deren Schutz zu treffen. Die Delegationsnorm von Artikel 12 Absatz 2 BÜPF an den Bundesrat wird insbesondere mit diesem und mit den weiteren Artikeln des 3. Abschnittes umgesetzt.

Nach *Buchstabe a* wird ein Zugriffs- und Änderungsschutz vorgenommen. Jede Person hat sich am V-FMÜ anzumelden und zu authentifizieren. Dies soll vor allem den unbefugten Zugriff und somit den Diebstahl oder die widerrechtliche Verwendung von Daten verhindern. Zudem haben die berechtigten Personen nur diejenigen Rechte (wie Lese- und Schreibrechte), die zur Erfüllung ihrer Aufgaben notwendig sind. Insbesondere sind die berechtigten Personen nicht berechtigt, irgendwelche Daten endgültig zu löschen. Die jeweiligen Rechte werden im Anhang aufgeführt. Sämtliche Daten des V-FMÜ werden gesichert, meist verschlüsselt, übermittelt. Unverschlüsselt werden Daten beispielsweise über gesicherte Glasfasernetze direkt ins V-FMÜ übermittelt.

Nach *Buchstaben b* schützt auch das V-FMÜ die Daten, indem es bei deren Transport darauf achtet, dass die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Deshalb werden die Daten des Verarbeitungssystems gesichert übermittelt.

Nach *Buchstaben c* soll auch die Kontrolle des Zugriffs und der Änderungen überprüft werden. Dazu werden sämtliche Änderungen, insbesondere nach Artikel 5, aber auch nur Lesezugriffe oder Suchen, protokolliert. Der Dienst ÜPF prüft die Daten sowie die Datenzugriffe regelmässig auf Unregelmässigkeiten, indem er Stichproben vornimmt. Dies kann beispielsweise auch durch Nachfragen bei den Strafverfolgungsbehörden geschehen.

Absatz 2 sieht vor, dass der Dienst ÜPF gestützt auf eine Risikoanalyse die zu treffenden Massnahmen bestimmt. Die Kontrollen sind je nach Benutzergruppe unterschiedlich und können unter anderem Zugangs-, Benutzer-, Zugriffs-, Transport- und Eingabekontrollen sein. Die Risikoanalyse führt der Dienst ÜPF nach Massgabe des Stands der Technik. Dieser ist vereinheitlicht in internationalen

Standards wie ETSI (European Telecommunications Standards Institute) festgelegt. Dabei handelt es sich um bereits erprobte Standards, die sowohl den Mitwirkungspflichtigen wie auch den Strafverfolgungsbehörden bekannt sind. Dies erleichtert eine bessere Qualität der Datenübermittlung und vereinfacht die komplizierten technischen Abläufe.

Absatz 3 beauftragt den Dienst ÜPF entsprechende Anweisungen zu technischen und organisatorischen Massnahmen zur Datensicherheit an sämtliche Systembenutzerinnen und -benutzer (des Dienstes ÜPF wie auch der Strafverfolgungsbehörden und der Mitwirkungspflichtigen) zu erlassen. Diese Anweisungen sind notwendig, damit die Daten, vor allem die besonders schützenswerten Personendaten, im V-FMÜ korrekt bearbeitet werden und somit geschützt sind und beispielsweise nicht widerrechtlich entwendet werden können. Dabei handelt es sich zum Beispiel um Angaben, wie die Daten bearbeitet werden dürfen, wie Vorzugehen ist bei Verlust eines Nummerntoken oder bei Abmelden eines Zugriffs.

Nach *Absatz 4* wird jede Bearbeitung von Daten im V-FMÜ, sämtliche Lesezugriffe und Suchen, die Wartung, der Unterhalt und der Support protokolliert. Die Protokolldaten sind alle geloggt. Mit anderen Worten bestehen Protokolldateien, in denen festgehalten wird, wo, wer, wann, was im V-FMÜ gemacht hat. Die Protokolle werden während der gesamten Speicherdauer der jeweiligen Daten aus Auskünften und Überwachungen vom Dienst ÜPF aufbewahrt.

Art. 11 Massnahmen für die Systemsicherheit

Bei drohender oder bestehender Störung des ordentlichen Betriebs, beispielsweise bei einer Systemüberlastung aufgrund einer Überwachungsmassnahme oder bei einem Systemabsturz, muss schnell gehandelt werden, weil sonst die Gefahr besteht, dass das System überhaupt nicht mehr verfügbar ist und somit etliche Daten verloren gehen. Sobald die Störung gefunden wurde, soll der Dienst ÜPF die anordnende (wie Staatsanwaltschaft) oder auswertende (wie Polizei) Behörde kontaktieren und die weiteren Massnahmen beraten. Dabei ist der Dienst ÜPF frei in der Entscheidung, ob er die anordnende oder auswertende Behörde kontaktiert. Nach deren Anhörung entscheidet der Dienst ÜPF über die zu treffenden Massnahmen. In Fällen, in welchen sofort gehandelt werden muss, kann der Dienst ÜPF auch ohne vorherige Kontaktaufnahme mit der anordnenden oder auswertenden Behörde entscheiden.

Art. 12 Anonymisierung

Daten können auch für die Statistik (Art. 12 VÜPF) verwendet werden. Sie sind allerdings zum Schutze der Personendaten vor ihrer Herausgabe zu anonymisieren. Nicht anonymisiert werden die Daten, welche an das Schweizerische Bundesarchiv übermittelt werden.

4. Abschnitt: Zugriff auf Überwachungsdaten im Abrufverfahren, Vernichtung und Archivierung der Daten

Art. 13 Zugriff auf Überwachungsdaten im Abrufverfahren

Artikel 11 BÜPF äussert sich allgemein zu den Aufbewahrungsfristen für Daten im V-FMÜ.

Absatz 1 bestimmt, dass die Überwachungsdaten, wozu auch die entsprechenden Daten der Geschäftsabwicklung und -kontrolle gehören, den Behörden bis zu einem maximalen Zeitpunkt zur Verfügung stehen. Nach *Buchstaben a* ist der maximale Zeitpunkt für ein Verfahren der rechtskräftige Entscheid, nach *Buchstaben b* für eine Operation des NDB deren Abschluss, nach *Buchstaben c* für die Notsuche und nach *Buchstaben d* für die Fahndung ebenfalls deren Abschluss. Nach *Buchstaben e* stehen den Behörden im Fall eines internationalen Rechtshilfeverfahrens die Überwachungsdaten maximal bis zum Versand der Datenträger oder Dokumente an die Behörde zur Übermittlung an die ausländische Behörde zur Verfügung (vgl. Art. 9 Abs. 4 BÜPF). Buchstaben d und e gelten auch im Falle einer Auslieferung und beschränken sich nicht nur auf die akzessorische (kleine) Rechtshilfe. Die bisherige Gesetzgebung sah vor, dass der Dienst ÜPF die Überwachungsdaten spätestens drei Monate nach der Einstellung der Überwachung vernichtet (Art. 10 Abs. 1 aVÜPF)¹⁴. In der Praxis zeigte sich jedoch, dass insbesondere die Polizei zur Auswertung der Daten wesentlich länger als drei Monate brauchen. Zudem kann die Bearbeitung der Daten auch während eines Instanzenzugs, wie vor einer zweiten Instanz oder dem Bundesgericht, benötigt werden. Im Schnitt würden die Daten somit ungefähr fünf Jahre bis zum rechtskräftigen Entscheid mit sämtlichen Bearbeitungsfunktionen zur Verfügung stehen. Die Behörde kann allerdings auch Anordnen, dass die Daten nicht mehr mit sämtlichen Bearbeitungsfunktionen benötigt werden, dann werden die Daten nach Absatz 3 über einen längeren Zeitraum im Verarbeitungssystem aufbewahrt. Dies dürfte mehrheitlich der Fall sein, da zwölf Monate nach Aufhebung der Überwachung (sog. Vorhaltefrist) alle drei Monate für jeweils die vollen drei Monate eine Gebühr für die Verlängerung des Zugriffs nach Artikel 11 GebV-ÜPF fällig wird. Die Behörden erhalten in der Regel (vgl. Art. 9 Abs. 4 BÜPF) mittels Abrufverfahren (Online-Zugriff) direkt oder über die Schnittstellen zum polizeilichen Informationssystem-Verbund des Bundesamtes für Polizei und zum Informationssystem des Nachrichtendienstes (Art. 9 Bst. b) Zugriff auf die Überwachungsdaten.

[Text zum NDG nur, wenn dieses vor dem BÜPF oder gleichzeitig mit diesem in Kraft tritt.]

Absatz 2 regelt, dass die Behörden im Falle umfassender technischer Änderungen am Verarbeitungssystemen die Daten während sechs bis zwölf Monaten noch mit sämtlichen Funktionen bearbeiten können. Die Beschränkung der weiteren Bearbeitungsmöglichkeit ist beispielsweise bei einem System- oder Lieferantenwechsel notwendig. Aber auch wenn sich die Daten strukturell grundlegend ändern, wie aufgrund eines wesentlichen Releasewechsels, können umfassende technische

¹⁴ Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001

Änderungen vorliegen. Unter Umständen müssten sonst um die Bearbeitungsfunktionen aufrechtzuerhalten, die alte Komponente noch über ein Jahr parallel zur neuen betrieben werden, was erheblichen Kosten verursachen würde. Deshalb sollen die Daten höchstens noch zwölf Monate mit allen Bearbeitungsfunktionen in der alten Komponente bearbeitet werden können. Es ist am Dienst ÜPF, in Absprache mit den Behörden, zu entscheiden, wie lange die Behörden noch auf die Daten mit sämtlichen Bearbeitungsfunktion zugreifen können (6-12 Monate) sowie wie mit den Daten weiter verfahren wird. Denkbar sind einerseits eine Datenmigration und andererseits die weitere Aufbewahrung mit verminderten Bearbeitungsfunktion nach Artikel 11 BÜPF.

Nach *Absatz 3* werden die Daten nach Rechtskraft des Entscheides mit verminderten Bearbeitungsfunktionen über einen längeren Zeitraum im V-FMÜ aufbewahrt. Die Behörde kann dem Dienst ÜPF allerdings auch vorher anordnen, dass sie die Daten nicht mehr mit sämtlichen Bearbeitungsfunktionen benötigt, so dass die Daten entsprechend aufbewahrt werden können. In letzterem Fall entfallen die entsprechenden Gebühren für die Speicherung mit sämtlichen Bearbeitungsfunktionen (Art. 11 GebV-ÜPF). Eine Behörde kann allerdings auch nach Rechtskraft des Entscheides die aufbewahrten Daten benötigen, dies kann beispielsweise der Fall sein bei der Wiederaufnahme des Verfahrens (Art. 323 StPO), der Revision (Art. 410 StPO) oder wenn die Daten in einem anderen Verfahren benötigt werden. Die Daten können diesfalls mit verminderten Funktionen, wie Lesen, Suchen, Filtern, selektives Herunterladen, bearbeitet werden. Zurzeit ist aufgrund des Standes des Projektes Programm FMÜ noch nicht klar, ob die verminderten Bearbeitungsfunktionen nur einem eingeschränkten Benutzerkreis zur Verfügung gestellt werden können. In diesem Fall würden den Behörden, die keinen Zugriff zu den über längeren Zeitraum aufbewahrten Daten haben, diese Daten zur Übertragung in ihr Ermittlungssystem zur Verfügung gestellt. Einen erneuten Online-Zugriff mit Bearbeitungsfunktionen ist nicht vorgesehen. Die unterschiedliche Aufbewahrungsfrist richtet sich nach Artikel 11 BÜPF.

Art. 14 Vernichtung

Nach *Absatz 1* hat die mit dem Verfahren befasste Behörde oder, wenn keine Behörde mehr mit dem Verfahren befasst ist, die zuletzt mit dem Verfahren befasste Behörde die Wahl, ob sie die Daten vor Ablauf der Aufbewahrungsfrist gemäss Artikel 11 BÜPF direkt vernichten lassen möchte oder ob die Daten vor der Vernichtung einer von ihr bezeichneten Behörde zur Verfügung gestellt werden sollen (z. B. für ihre Archivierung; siehe Art. 15). Die Daten würden der Behörde analog Artikel 9 Absatz 4 BÜPF zur Verfügung gestellt, das heisst sie würden nach Möglichkeit verschlüsselt, mittels Datenträgern oder Dokumenten auf dem Postweg zugestellt. Die entsprechenden Daten der Geschäftsabwicklung und -kontrolle werden im System ebenfalls vernichtet. Es kann durchaus sein, dass es nach der längeren Zeit der Aufbewahrungsdauer einer zuletzt mit dem Verfahren befasste Behörde entgeht, sich beim Dienst ÜPF zu melden. Dann nimmt der Dienst ÜPF mit dieser Behörde Kontakt auf und erkundet sich nach dem weiteren Vorgehen. Damit kommt der Dienst ÜPF auch der Pflicht nach Artikel 11 Absatz 5 letzter

Satz BÜPF nach, wonach er sich nach 30 Jahren nach Abschluss der Überwachung bei der mit dem Verfahren befassten Behörde zu erkunden hat.

Damit die Daten im V-FMÜ nach Ablauf der Aufbewahrungsfrist auch vernichtet werden können, wenn die zuständige Behörde nicht mehr eruierbar ist oder keine Instruktion gibt, hält *Absatz 2* fest, dass der Dienst ÜPF die Möglichkeit hat, die Daten auf einen Datenträger zu speichern und diesen für kantonale Verfahren der obersten kantonalen gerichtlichen Behörde des jeweiligen Kantons und für Verfahren von Bundesbehörden dem Bundesstrafgericht zukommen zu lassen. Dieser Vorgang ist zu protokollieren. Nach Erhalt der Lesbarkeitsbestätigung können die Daten im V-FMÜ vernichtet werden.

Absatz 3 hält fest, dass die Auskünfte zwölf Monaten gespeichert und anschliessend gelöscht werden. Sie werden nicht zentral für längere Zeit aufbewahrt. Auskünfte sind verschiedenste einfachere Informationen, welche den Strafverfolgungsbehörden Anhaltspunkte für die weiteren Ermittlungen geben sollen. Die Strafverfolgungsbehörden können diese in andere Ermittlungsdokumente aufnehmen und so dem Strafdossier zufügen.

Art. 15 Archivierung

Da in der Regel¹⁵ nicht der Dienst ÜPF Datenherr ist, sondern die anordnende Behörde, richtet sich die Archivierung der Daten nach den unterschiedlichen Rechtsgrundlagen der Datenherren.

Absatz 1 bestimmt das Vorgehen bei Daten des Bundes, welche sich nach der Archivierungsgesetzgebung des Bundes richtet. Nach dem Bundesgesetz vom 26. Juni 1998¹⁶ (Archivierungsgesetz, BGA) ist der Dienst anbietepflichtig und das Bundesarchiv legt in Zusammenarbeit mit dem Dienst fest, ob Unterlagen archivwürdig sind. Der Dienst bereitet die archivwürdigen Daten gemäss Artikel 5 Absatz 1 der Archivierungsverordnung vom 8. September 1999¹⁷ (VBGA) sowie in Verbindung mit Artikel 5 Absatz 1 und Artikel 8 der Weisung vom 28. September 1999 über die Anbietepflicht und die Ablieferung von Unterlagen an das Schweizerische Bundesarchiv¹⁸ auf. Nicht archivwürdige Daten werden gemäss den Fristen nach Artikel 11 BÜPF vernichtet.

Absatz 2 bestimmt das Vorgehen bei Daten der Kantone und verweist auf Artikel 4 Absatz 2 BGA und hält fest, dass bei Daten, wo eine kantonale Behörde Datenherr ist, das kantonale Recht zur Anwendung kommt. Der Datenherr, wie die kantonale Strafbehörde, bietet der zuständigen kantonalen Behörde die Daten zur Archivierung an.

¹⁵ vgl. den Kommentar zu Artikel 6 VVS-ÜPF

¹⁶ SR 152.1

¹⁷ SR 152.11

¹⁸ <https://www.bar.admin.ch/bar/de/home.html>

5. Abschnitt: Schlussbestimmung

Art. 16 Übergangsbestimmung

Absatz 1 soll dem Dienst ÜPF die Möglichkeit geben, die Protokollierungen noch nach altem Recht vorzunehmen bis die Systemkomponenten nach der Etappe 1 des Programms zum Ausbau und zum Betrieb des V-FMÜ zur Fernmeldeüberwachung sowie der polizeilichen Informationssysteme des Bundes (Programm FMÜ)¹⁹ in Betrieb genommen wurden. Die alten Systeme, vor allem das CCIS, bei welchem der Wartungsvertrag nicht mehr angepasst werden kann, ermöglichen nicht die gewünschten Protokollierungen.

Die Langzeitaufbewahrung ist erst noch zu planen und umzusetzen, weshalb *Absatz 2* eine Übergangsbestimmung vorsieht. Zum heutigen Zeitpunkt ist nicht klar, ob diese bereits mit Inkrafttreten des Gesetzes und der entsprechenden Ausführungsverordnungen in Betrieb sein wird. Deshalb werden die Daten wie bisher den anordnenden Behörde oder einer von ihr benannten auswertenden Behörde auf einem Datenträger zur Verfügung gestellt (vgl. Art. 19 Abs. 4 GebV-ÜPF) oder sofern technisch bereits im V-FMÜ möglich, können sie die Daten in ihr System herunterladen.

Art. 17 Inkrafttreten

Diese Verordnung tritt mit dem totalrevidierten Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs und allen übrigen Ausführungsverordnungen in Kraft.

¹⁹ BBl 2014 6711