Bern, 15. November 2023

Teilrevisionen von Ausführungserlassen des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Erläuterungen

Inhaltsverzeichnis

1 Ausgangslage 3

2 Vorverfahren, insbesondere Vernehmlassungsverfahren 3

3 Grundzüge der Vorlage 6

3.1 Anpassungen der VÜPF 6

3.2 Anpassungen der GebV-ÜPF 8

3.3 Anpassungen der VD-ÜPF 8

3.4 Anpassungen der VVS-ÜPF 8

4 Erläuterungen zu einzelnen Artikeln 8

4.1 Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) 8

4.2 Verordnung über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) 57

4.3 Verordnung über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (VVS-ÜPF) 61

5 Auswirkungen 66

5.1 Auswirkungen auf den Bund 66

5.2 Auswirkungen auf Kantone 66

5.3 Auswirkungen auf die MWP 66

6 Rechtliche Aspekte 66

6.1 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz 66

6.2 Erlassform 67

6.3 Subdelegation von Rechtsetzungsbefugnissen 67

6.4 Datenschutz 67

Anhang 67

Tabelle «Übersicht Bearbeitungszeiten» 69

1 Ausgangslage

Die Ausführungserlasse zum BÜPF[1] zeigen aktuell folgenden Revisionsbedarf:

- Anlässlich der Änderung vom 22. März 2019 des FMG[2] wurde ein zusätzlicher Absatz 2 zu Artikel 2 BÜPF eingefügt. Dieser neue Absatz ermächtigt den Bundesrat, die Kategorien von Mitwirkungspflichtigen (MWP) näher zu umschreiben, insbesondere jene nach Artikel 2 Buchstaben b, c und e BÜPF (AS 2020 6159, 6181).
- Die 5G-Technologie erfordert Anpassungen in der VÜPF[3], zudem sind Massnahmen zur Verbesserung und Sicherstellung der generellen Datenlieferung notwendig. Weiter sind einige Bestimmungen der GebV-ÜPF[4], der VD-ÜPF[5] und der VVS-ÜPF[6] anzupassen.

Um die Anpassungen an die 5G-Technologie nicht zu verzögern, wird die Revision in zwei Schritten erfolgen. Nicht Bestandteil des vorliegenden ersten Revisionspakets ist die Definition der verschiedenen Kategorien der MWP und ihrer Pflichten. Dies wird in einer zweiten, nachfolgenden Revision angegangen. Die vorgesehene Totalrevision der GebV-ÜPF, welche die Pauschalen einführt (vgl. Art. 38*a* BÜPF, in Kraft seit dem 01.01.2022), erfolgt in einer weiteren separaten Vorlage, die Verordnung über die Finanzierung der Überwachung des Post- und Fernmeldeverkehrs (FV-ÜPF).

Die vorliegende Vorlage wird an die technologischen Fortschritte wie die 5G-Technologie und das IP Multimedia Subsystem (IMS) angepasst (s. unten Ziff. 3.1).

2 Vorverfahren, insbesondere Vernehmlassungsverfahren

Vom 16. Februar bis 23. Mai 2022 wurde ein Vernehmlassungsverfahren durchgeführt. Das EJPD (Dienst ÜPF) hat 70 Antworten erhalten.

Es wurden zwei entgegenstehende Meinungen vertreten: Die Kantone und die Strafverfolgungsbehörden begrüssten die Vorlage grundsätzlich. Die Organisationen der Telekommunikation und die MWP kritisierten diese hingegen stark oder lehnten diese teilweise ab. Sie monieren, dass nicht nur Bestimmungen im Zusammenhang mit der 5G-Technologie geändert würden, sondern auch andere, welche eine Ausweitung der allgemeinen Überwachung darstellen. Speziell kritisiert wurden die zusätzliche Automatisierung, das Virtual Private Network (virtuelles privates Netzwerk, kurz: VPN),

1 Bundesgesetz vom 18.03.2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (**BÜPF**; SR **780.1**)
2 Fernmeldegesetz vom 30.04.1997 (**FMG**; SR **784.10**)
3 Verordnung vom 15.11.2017 über die Überwachung des Post- und Fernmeldeverkehrs (**VÜPF**, SR **780.11**)
4 Verordnung vom 15.11.2017 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (**GebV-ÜPF**, SR **780.115.1**)
5 Verordnung des EJPD vom 15.11.2017 über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (**VD-ÜPF**, SR **780.117**)
6 Verordnung vom 15.11.2017 über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (**VVS-ÜPF**, SR **780.12**)

die Entfernung der durch die Anbieterin angebrachte Verschlüsselung, die Speicherung der Ports, IP-Adressen und anderen Daten (die als Vorratsdatenspeicherung angesehen wird)[7], die Lokalisierung (LALS), der Zeitstempel, die kürzere Ausführungsfristen und die zu kurzen Übergangsfristen. Hinter der Ankündigung der Anpassung an die technologischen Entwicklungen würde sich ein massiver Ausbau der Überwachungen verbergen. Zusammengefasst würden diese Erweiterungen der Mitwirkungspflichten den Unternehmen unverhältnismässige, neue Belastungen aufbürden und die Privatsphäre und den Datenschutz der Nutzer einschränken.

Folgende Punkte aus der Vernehmlassung wurden bei der Überarbeitung der Vorlage berücksichtigt:

- Bestimmungen wurden angepasst oder ganz gestrichen, damit der den MWP durch die Änderungen der Verordnungen generierte Aufwand (insb. Anpassung der Systeme) in einem vertretbaren Verhältnis zum Nutzen der Strafverfolgungsbehörden steht (Verhältnismässigkeit der Änderungen).
- Etliche Vernehmlassungsteilnehmende haben die Speicherung der Ziel-Portnummern und Ziel-IP-Adressen kritisiert. Sie bringen insbesondere vor, dass die Speicherung dieser Daten einer Ausweitung der Überwachung gleichkomme, für diese keine Rechtsgrundlage bestehe und sie datenschutzrechtlich problematisch sei. Die neue Pflicht zur Lieferung der Ziel-Adressierungselemente (Ziel-NAT) wird in die zweite Revision verschoben, damit die Kategorien von MWP und die entsprechenden Pflichten gleichzeitig eingeführt werden. Vorliegend handelt es sich um eine Auskunft und nicht um eine Überwachung. Die Auskünfte nach Artikel 22 BÜPF dürfen sich auch auf Randdaten stützen, sofern es zur Identifikation notwendig ist. Die Randdaten selbst werden dabei nicht herausgegeben. Ausserdem werden die Anbieterinnen angehalten, ein Verfahren zu wählen, bei dem Ziel-IP-Adressen und -Ports nicht zur Identifikation der Benutzerschaft erforderlich sind, so dass diese auch nicht gespeichert werden müssen. Das BÜPF (insb. Art. 21 und 22) stellt eine genügende Rechtsgrundlage dar. Selbst wenn es sich um eine Überwachung handeln würde, würde Artikel 269 StPO[8] keine entsprechende Einschränkung vorsehen.
- Der Absatz in Artikel 50, der die Entfernung der angebrachten Verschlüsselungen für die AAKD mit weitergehenden Pflichten vorsah, wurde gestrichen. Für die FDA gilt die Entfernung der Verschlüsselung weiterhin nach Artikel 26 Absatz 2 Buchstabe c BÜPF.
- Die Übergangssfristen für die Anpassung der Systeme der MWP wurden verlängert (24 Monate ab Inkrafttreten der VÜPF).
- Die Gebühren der neuen Überwachungstypen der Positionsbestimmung wurden leicht reduziert. Weiter wurde auch die Gesamtgebühr beim Auskunftstyp in Zusammenhang mit einem IMSI-Catcher-Einsatz (z. B. bei Notsuchen) herabgesetzt (s. Ziff. 3.2).

7 Betrifft die Änderungen in den Artikeln 21, 38, 42*a*, 43, 43*a*, 60, 62 und 63 VÜPF.
8 Schweizerische Strafprozessordnung vom 05.10.2007 (Strafprozessordnung, **StPO**; SR **312.0**)

Folgende Punkte aus der Vernehmlassung konnten bei der Überarbeitung der Vorlage nur teilweise berücksichtigt werden:

- Die MWP und einzelne politische Parteien kritisierten, dass neben den Anpassungen an die 5G-Technologie auch weitere Änderungen vorgenommen worden seien, welche einen massiven Ausbau der Überwachung mit zusätzlichen Pflichten für die MWP darstellen würden. Besonders kritisiert wurden die zur Identifikation der Teilnehmenden notwendigen Daten, die automatisierte Erteilung von Auskünften, die Positionsbestimmung und die kürzeren Bearbeitungsfristen (speziell zu diesen Punkten wird auf die folgenden Ausführungen verwiesen). Dieser allgemeinen Kritik ist zu entgegnen, dass es mit den Anpassungen an die 5G-Technologie für die Überwachungen neue Möglichkeiten geben wird (z. B. Lokalisierung). ETSI-Standards wurden dementsprechend auch bereits geändert. Ziel der zahlreichen Änderungen in den Verordnungen und insbesondere in der VÜPF ist, diese der technologischen Entwicklung anzupassen, damit keine Überwachungslücken entstehen. Auch die durch die 5G-Technologie verbesserten Lokalisierungsmöglichkeiten dienen einer besseren Qualität der Überwachungsdaten. Einige Anpassungen stellen eine Verbesserung der Teilnehmeridentifikation dar, und nicht zusätzliche Pflichten. Die Kritik wurde aber teilweise berücksichtigt: Einerseits wurde in verschiedenen Bestimmungen der Vorlage präzisiert, dass die AAKD mit weitergehenden Pflichten durch die neuen Auskunfts- und Überwachungstypen nicht betroffen sind und somit keine entsprechenden Pflichten haben; anderseits werden einige Änderungen betreffend die Pflichten der MWP in die zweite Revision verschoben, wie die neuen Auskunftstypen zur Identifikation der Benutzerschaft gemäss Artikel 42*a* und 43*a* VÜPF. So können die neuen Pflichten gleichzeitig mit der näheren Umschreibung der entsprechenden Kategorien von MWP eingeführt werden.
- Die MWP forderten, dass die automatisierte Erteilung der Auskünfte als Option vorgesehen und nicht zwingend vorgeschrieben wird. Dieser Forderung wird insofern nachgekommen, als sich die Pflicht zur automatisierten Erteilung nur auf diejenigen MWP beschränkt, welche heute schon die Auskünfte automatisiert erteilen und somit die dafür notwendigen Investitionen bereits gemacht haben. Der Auskunftstyp IR_13_EMAIL (Auskünfte über Teilnehmende von E-Mail-Diensten) ist neu manuell zu beantworten, da es für die MWP mit den neuen eingeführten Anforderungen zu komplex wäre, diesen automatisiert zu erteilen. Der neue Auskunftstyp IR_52_ASSOC_TEMP (sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren) muss hingegen automatisiert erteilt werden, weil die Daten unmittelbar zur Verfügung stehen müssen und dies mit einer manuellen Erteilung nicht umgesetzt werden kann.
- Die Regelung betreffend die Positionsbestimmung wurde auf die 5G-Technologie beschränkt und die Frist für die Implementierung von 12 beziehungsweise 18 auf 24 Monate verlängert.

Folgende Punkte aus der Vernehmlassung konnten bei der Überarbeitung der Vorlage nicht berücksichtigt werden:

- Einige Kantone sowie die KKPKS forderten technologieneutrale Formulierungen in den Verordnungen. Die technischen Details sollen in Anhänge oder

Weisungen verschoben werden, damit sie schnell angepasst werden können. Nur einzelne Bestimmungen technologieneutral zu formulieren, würde das Gesamtkonzept der VÜPF stören und sie unverständlicher machen. Deshalb kann dieses Anliegen nur mit einer Totalrevision der VÜPF umgesetzt werden. Da dies die Anpassungen an die 5G-Technologie zu sehr verzögern würde, wird dieses Anliegen bei der nächsten Revision erneut geprüft.

- Die MWP bemängelten die Verkürzung der Bearbeitungsfristen für die Beantwortung gewisser Auskunftstypen. In der Praxis wurde die Frist von einem Arbeitstag von den auskunftsberechtigten Behörden als zu lang erachtet, wenn ihre Anfrage während einem Wochenende oder einem Feiertag gestellt wurde. Die Frist von einem Arbeitstag kann dazu führen, dass die Auskunft zu spät kommt, was in gewissen dringenden Fällen verheerende Folgen haben kann, so bei anonymen Bombendrohungen. Die entsprechende Kürzung der Frist in der VD-ÜPF erscheint deshalb als angemessen, auch da sie nur für ausserhalb der Normalarbeitszeiten und an Feiertagen eingegangene Auskünfte gilt.
- Viele Anbieterinnen, aber auch weitere Organisationen, forderten eine höhere Entschädigung der MWP, während vier Kantone deren Senkung beantragten. Die MWP erachteten insbesondere die Entschädigungen in der Höhe von drei Franken für alle einfachen Auskünfte als zu tief. Im Urteil vom 27. Juli 2021 (2C_650/2020) hat das Bundesgericht jedoch entschieden, dass eine Entschädigung in der Höhe von drei Franken für die Beantwortung eines Auskunftsgesuches IR_7_IP (Art. 37 VÜPF) angemessen im Sinne von Artikel 38 Absatz 2 BÜPF ist. Auf dieses Anliegen wird nicht weiter eingegangen, weil die Gebühren und Entschädigungen der neuen Auskunfts- und Überwachungstypen ebenfalls von der FV-ÜPF, die die Pauschalen einführt, geregelt werden.

3 Grundzüge der Vorlage

3.1 Anpassungen der VÜPF

Die VÜPF wird an die technologischen Fortschritte wie die 5G-Technologie und das IMS angepasst.

In der VÜPF werden drei neue Auskunfts- und vier neue Überwachungstypen geschaffen:

- den Auskunftstyp IR_51_ASSOC_PERM, Auskünfte über längerfristig zugeordnete Identifikatoren (Art. 48*a* VÜPF);
- den Auskunftstyp IR_52_ASSOC_TEMP, sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren (Art. 48*b* VÜPF);
- den Auskunftstyp IR_53_TEL_ADJ_NET, Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten (Art. 48*c* VÜPF);
- den Überwachungstyp (Echtzeitüberwachung) RT_54_POS_ONCE, einmalige, sofortige Positionsbestimmung durch das Netzwerk (Art. 56*a* VÜPF);
- den Überwachungstyp (Echtzeitüberwachung) RT_55_POS_PERIOD, periodisch wiederkehrende Positionsbestimmung durch das Netzwerk (Art. 56*b* VÜPF);

- den Überwachungstyp (Notsuche) EP_56_POS_ONCE, einmalige, sofortige Positionsbestimmung durch das Netzwerk (Art. 67 Bst. b VÜPF); sowie
- den Überwachungstyp (Notsuche) EP_57_POS_PERIOD, periodisch wiederkehrende Positionsbestimmung durch das Netzwerk (Art. 67 Bst. c VÜPF).

Der neue Auskunftstyp IR_51_ASSOC_PERM wird geschaffen, um die zu einem Identifikator längerfristig zugeordneten Identifikatoren im IMS zu erhalten. Der neue Auskunftstyp IR_52_ASSOC_Temp wird eingeführt, um den zu einem temporären Identifikator der 5G-Technologie zugehörigen permanenten Identifikator automatisiert und echtzeitnah abfragen zu können, dies im Rahmen eines Einsatzes besonderer technischer Geräte zur Überwachung des Fernmeldeverkehrs (Art. 269bis StPO; sogenannte IMSI-Catcher). Der neue Auskunftstyp IR_53_TEL_ADJ_NET wird neu geschaffen, um spezifische Probleme der Identifikation der Täterschaft zu lösen, wie sie bei gefälschter (Spoofing) oder unbekannter Telefonnummer des Anrufers oder Absenders der Mitteilung auftreten. Dies kann zum Beispiel bei anonymen Bombendrohungen nützlich sein, um die Spur des anonymen Anrufs oder der anonymen Mitteilung nachverfolgen zu können. Die vier neuen Überwachungstypen werden geschaffen, um die neuen technischen Möglichkeiten des «Lawful Access to Location Services» (LALS) zur Positionsbestimmung im Mobilfunk zu nutzen. Sie erlauben die einmalige oder die periodisch wiederkehrende Positionsbestimmung durch das Netzwerk als Echtzeitüberwachung oder als Notsuche (Art. 56*a* und 56*b* bzw. für die Notsuche Art. 67 Bst. b und c).

Der neue Artikel 4*a* VÜPF legt die Regel des «dies a quo» für die Berechnung der Frist von 6 Monaten für rückwirkende Überwachungen fest. Die Berechnung dieser Frist war bisher in der Praxis umstritten.

Der bisherige Artikel 18 VÜPF wird für die bessere Lesbarkeit neu in vier Artikel (Art. 18, 18*a*, 18*b* und 18*c*) aufgeteilt. In diesen Artikeln werden die Pflichten im Zusammenhang mit der Auskunftserteilung näher ausgeführt. Es wird präzisiert, dass die in Absatz 1 erwähnten MWP die aufgeführten Auskünfte automatisiert erteilen müssen, während sie bei den anderen Auskünften die Wahl zwischen manueller und, im Einvernehmen mit dem Dienst ÜPF, automatisierter Erteilung haben.

Artikel 20 VÜPF (Erfassung von Angaben zur Person bei Mobilfunkdiensten) wird ergänzt und neu strukturiert in Bestimmungen für natürliche und juristische Personen. Artikel 20*c* VÜPF regelt neu die Abgabe von Zugangsmittel und Diensten an Polizeibehörden von Bund und Kantonen sowie den Nachrichtendienst des Bundes (NDB), wenn nur wenige Personen davon Kenntnis haben sollen. Die Identitätsprüfung war nach bisherigem Artikel 20 für alle Teilnehmenden vorgesehen, so auch für Angehörige der Polizeibehörden und Mitarbeitende des NDB. In der Praxis hat sich diese Regelung in den letzten Jahren für diese Behörden als besonders problematisch erwiesen.

Zur Gewährleistung einer einwandfreien Einführung der neuen Auskunfts- und Überwachungstypen bei den MWP und dem Dienst ÜPF sieht Artikel 74*b* VÜPF detaillierte Übergangsbestimmungen für die einzelnen Änderungen vor.

3.2 Anpassungen der GebV-ÜPF

Infolge der Einführung der neuen Auskunfts- und Überwachungstypen in der VÜPF wurde auch der Anhang der GebV-ÜPF entsprechend angepasst. Die Gebühren und Entschädigungen der anderen Auskunfts- und Überwachungstypen bleiben unverändert. Da vorgesehen ist, die FV-ÜPF und die vorliegende Revision gleichzeitig auf den 1. Januar 2024 in Kraft treten zu lassen, ist auf die Änderung der GebV-ÜPF zu verzichten. Notwendige Änderungen werden im Entwurf der FV-ÜPF berücksichtigt.

3.3 Anpassungen der VD-ÜPF

Mit der Revision der VD-ÜPF werden Bearbeitungsfristen für Auskünfte (Art. 14 VD-ÜPF) leicht geändert, um dem dringenden Bedürfnis der Strafverfolgungsbehörden nach kürzeren Fristen Rechnung zu tragen. Ausserdem werden im Geltungsbereich der VD-ÜPF neu ebenfalls die Behörden (im Sinne von Art. 1 Abs. 2 Bst. a-f VÜPF) aufgeführt. Somit gilt der geänderte Artikel 3 VD-ÜPF, der die gesicherte Kommunikation regelt, nun auch für die Behörden.

3.4 Anpassungen der VVS-ÜPF

Mit der vorliegenden Vorlage wird die Gelegenheit genutzt, auch einige Bestimmungen der VVS-ÜPF zu revidieren. Neben den Zugriffen auf die Anzeige der Betriebslage der Überwachungskomponente des Verarbeitungssystems (sog. «PTSS-Dashboard») werden auch die Zugriffe des Dienstes ÜPF auf Daten im Verarbeitungssystem (Art. 8 Abs. 3-6) sowie die Aufbewahrungsdauer der Protokolle der Vernichtung der Daten (Art. 10 Abs. 4) neu geregelt.

4 Erläuterungen zu einzelnen Artikeln

4.1 Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)

Vorbemerkung

Im Verordnungstext werden die Formulierungen «gegebenenfalls», «falls verfügbar», «soweit verfügbar», «falls vorhanden», «falls bekannt», «soweit bekannt», «falls zutreffend», «soweit zutreffend» und «soweit möglich» verwendet. Diese Formulierungen bringen zum Ausdruck, dass die entsprechenden Regelungen im jeweiligen Kontext zu betrachten sind und optionale Parameter oder Funktionen, bestimmte Technologien, Funktionen, Standards oder Versionen von Standards betreffen, auf deren Einzelheiten auf Verordnungsstufe der VÜPF nicht näher eingegangen werden kann. Auf Anfrage des Dienstes ÜPF haben die Anbieterinnen im Rahmen ihrer Mit-

wirkungspflichten eine ausführliche Begründung zu liefern, warum bestimmte Parameter, Daten und Funktionen nicht vorhanden sind respektive nicht geliefert werden können.

Ersatz von Ausdrücken

Nach *Absatz 1* wird der Begriff «WLAN-Zugangspunkt» an den entsprechenden Stellen durch den allgemeineren Begriff «WLAN-Zugang» ersetzt, da dieser sowohl Zugangspunkte als auch Hotspots einschliesst. Diese Anpassung ist angebracht, da es sich in der Praxis gezeigt hat, dass die Identifikation eines bestimmten WLAN-Zugangs oft nicht auf der Ebene des Zugangspunkts (*access point*) möglich ist, sondern nur auf der Ebene des Hotspots.

Absatz 2 hält fest, dass die Überarbeitung zum Anlass genommen wird, in der VÜPF die Abkürzung *AAKD* (Anbieterinnen abgeleiteten Kommunikationsdienste; Art. 2 Bst. c BÜPF) aufzunehmen, die bereits in der Praxis zusammen mit der Abkürzung *FDA* (Anbieterinnen von Fernmeldediensten; Art. 2 Bst. b BÜPF) verwendet wird (s. auch die Änderung in Art. 1 Abs. 2 Bst. j).

Absatz 3 betrifft den Begriff «überwachten Identifikator (Target-ID)», der in «Target-ID» abgekürzt werden kann.

Art. 1 Abs. 1 und Abs. 2 Bst. j

In *Absatz 1* wird vor dem Wort «Erteilung» die Präposition «zur» eingefügt. Diese redaktionelle Anpassung dient zur Klarstellung, dass sich «die Organisation und das Verfahren» auch auf die Erteilung von Auskünften bezieht.

In *Absatz 2 Buchstabe j* wird die Abkürzung *AAKD* eingefügt (vgl. die in Bst. i bereits verwendete Abkürzung *FDA*). Die aus dem Gesetzestext (Art. 2 Bst. c BÜPF) übernommene Passage «Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen» entfällt, um eine unnötige Wiederholung des Gesetzestextes in der Verordnung zu vermeiden. Für AAKD, die sowohl weitergehende Auskunftspflichten (Art. 22) als auch weitergehende Überwachungspflichten (Art. 52) haben, wird die Schreibweise *AAKD mit weitergehenden Pflichten* verwendet. Der materielle Gehalt der Bestimmung ändert sich nicht.

Art. 3 **Eingaben beim Dienst ÜPF**

Der Einleitungssatz wird angepasst, um auch die Übermittlungen der Genehmigungsbehörden zu regeln. Eine mögliche Erfassung im Abrufverfahren der Überwachungsgenehmigung und allfälliger Auflagen durch die Genehmigungsbehörde wird durch diese Bestimmung auch abgedeckt. Die Genehmigung gehört zur Geschäftsabwicklung und -kontrolle gemäss Artikel 6 Buchstabe f VVS-ÜPF in Verbindung mit Artikel 7 Buchstabe e BÜPF.

In *Buchstabe a* wird das zugelassene sichere Übertragungsmittel neu nicht mehr durch den Dienst ÜPF, sondern durch das EJPD bestimmt, und zwar in Artikel 3 VD-ÜPF (Departementsverordnung). Da das Telefax technologisch überholt ist und nicht mehr

den heutigen Sicherheitsstandards entspricht, sieht *Buchstabe b* es neu nicht mehr vor. Der *Buchstabe c* enthält keine materiellen Änderungen.

Da heute der Online-Zugriff standardmässig zur Anwendung kommt, ist der bisherige *Absatz 2* nicht mehr aktuell und wird deswegen nicht übernommen.

Art. 4a Beginn und Ende der rückwirkenden Überwachung

Der neue Artikel 4*a* gilt sowohl für den Post- als auch für den Fernmeldeverkehr, deshalb befindet sich diese Bestimmung im 2. Abschnitt «Überwachungsanordnung».

Die maximale Dauer einer rückwirkenden Überwachung ist im Gesetz festgelegt. Die anordnende Behörde kann auch eine kürzere Überwachungsdauer in der Anordnung vorsehen. Randdaten können unabhängig von der Dauer der Überwachung bis 6 Monate rückwirkend verlangt werden (Art. 273 Abs. 3 StPO). Dafür müssen die betroffenen Anbieterinnen die Randdaten des Post- und Fernmeldeverkehrs (Art. 19 Abs. 4 und Art. 26 Abs. 5 BÜPF) sowie die Randdaten zum Zweck der Identifikation (Art. 21 Abs. 5 VÜPF i. V. m. Art. 21 Abs. 2 und Art. 22 Abs. 2 BÜPF) während 6 Monaten aufbewahren. Was die Frist von 6 Monaten in der Praxis genau für den Beginn und das Ende einer rückwirkenden Überwachung bedeutet und wie sie zu berechnen ist, wurde bis jetzt nicht im Einzelnen in einer Verordnung festgelegt, was wiederholt zu Diskussionen geführt hat.

Im neuen *Absatz 1* wird die Regel des «dies a quo» für die Berechnung der Frist von 6 Monaten für rückwirkende Überwachungen festgelegt. Der für die Berechnung massgebliche Tag ist der Tag des Empfangs der Anordnung durch den Dienst ÜPF. Somit ist nicht das Datum der Anordnung oder der Übermittlung[9] durch die anordnende Behörde massgebend.

Der Tag des Empfangs der Anordnung wird dem Tag der Übermittlung der Anordnung aus nachfolgenden Gründen vorgezogen: Bei der üblichen Übermittlung über die Auftragsmanagementkomponente WMC[10] macht es keinen Unterschied, ob die Berechnung der Frist auf den Tag der Übermittlung oder des Empfangs abstellt. Der Zeitabstand zwischen der Übermittlung der Anordnung durch die anordnende Behörde und dem Empfang durch den Dienst ÜPF ist vernachlässigbar, da dies nur wenige Sekunden dauert. Nur beim Postversand der Anordnung, was nur in Ausnahmefällen erfolgt, wenn ein durch das EJPD zugelassenes sicheres Übertragungsmittel aus technischen Gründen nicht zur Verfügung steht (Art. 3 VÜPF), ergibt sich eine grössere Verzögerung von einem oder gar mehreren Tagen (s. u. Bsp. 4). Die anordnende Behörde kann diese Verzögerung vermeiden, indem sie die Anordnung gemäss Artikel 3 Buchstabe c telefonisch an den Dienst ÜPF übermittelt. Bei telefonischer Beauftragung gilt der Zeitpunkt des Anrufs und nicht der Zeitpunkt des Empfangs der schriftlich nachgereichten Anordnung (s. u. Bsp. 3).

9 Als Übermittlung gilt einer der in Artikel 3 VÜPF vorgesehenen Übermittlungswege (SYLVAIN Métille, in KUHN/ JEANNERET, Commentaire romand du Code de procédure pénale suisse, Helbling Lichtenhahn, 2. Auflage 2019, Basel, ad Art. 274, S. 1794, RZ 12)

10 Warrant Management Component (WMC); Komponente des Verarbeitungssystems des Dienstes ÜPF (s. das Programm FMÜ), in Betrieb seit dem 18.03.2019.

Ein Zeitabstand von einem oder mehreren Tagen zwischen der Übermittlung der Anordnung durch die Behörde und der Auftragserteilung an die Anbieterin durch den Dienst ÜPF wäre problematisch, da die Anbieterinnen auch verpflichtet sind, die historischen Daten nach Ablauf der Aufbewahrungsfrist von 6 Monaten zu löschen (Art. 21 Abs. 7). Wie das Beispiel 4 zeigt, besteht somit das Risiko, dass die ältesten der von den anordnenden Behörden verlangten Daten durch die Anbieterinnen bereits gelöscht sind, wenn der Überwachungsauftrag bei der Anbieterin eintrifft. Der Dienst ÜPF garantiert, dass die Zeit zwischen dem Eingang der Anordnung beim Dienst ÜPF und der Erteilung der entsprechenden Aufträge an die Anbieterinnen nur maximal eine Stunde beträgt. Da der Zeitpunkt des Empfangs der Anordnung massgeblich ist für die Berechnung des frühestmöglichen Beginns der rückwirkenden Überwachung, entsteht somit kein Konflikt für die Anbieterinnen zwischen Aufbewahrung und Löschung der Randdaten.

Zu beachten ist, dass mit dem Zeitpunkt der Übermittlung der Anordnung durch die anordnende Behörde an den Dienst ÜPF die Frist von 24 Stunden zur Einreichung der Unterlagen an das Zwangsmassnahmengericht gemäss Artikel 274 Absatz 1 StPO zu laufen beginnt[11].

Im Normalfall wird die Anordnung in der Auftragsmanagementkomponente (WMC) des Verarbeitungssystems des Dienstes ÜPF hochgeladen und die Übermittlung durch die anordnende Behörde und der Empfang durch den Dienst ÜPF erfolgen am gleichen Tag (s. u. Bsp. 2).

Die rückwirkende Überwachung beginnt somit frühestens 6 Monate vor dem Tag des Empfangs der Anordnung durch den Dienst ÜPF. Zur Erinnerung: Artikel 273 Absatz 3 StPO sieht eine Frist in Monaten und nicht in Tagen oder Stunden vor.

Die Berechnung der Frist von 6 Monaten richtet sich nach der Lehre[12] und der Rechtsprechung[13]: «Die in Monaten festgesetzte Frist endet an dem Tag, der im Kalender dem Tag des Ereignisses, sprich derselben Ziffer des Tages, entspricht, das sie ausgelöst hat, oder, mangels eines entsprechenden Tages, am letzten Tag des Monats.»[14] In anderen Worten bedeutet das für die rückwirkende Überwachung, dass eine in Monaten festgesetzte Frist an demjenigen Tag beginnt, der durch seine Zahl dem Tag des Empfangs der Anordnung durch den Dienst ÜPF entspricht. Der Tag des Beginns der rückwirkenden Überwachung hat in der Regel die gleiche Zahl wie der Tag (TT) des Datums (TT.MM.JJJJ) des Empfangs der Anordnung durch den Dienst ÜPF.

Der besondere Fall, wenn der entsprechende Tag im Monat des Beginns der rückwirkenden Überwachung fehlt, das heisst wenn dieser Monat kürzer ist, als der Monat der Anordnung, wird im *zweiten Satz* geregelt. Wenn beispielsweise die Anordnung

11 MARC JEAN-Richard-DIT-BRESSEL, in Basler Kommentar, NIGGLI, HEER, WIPRÄCHTIGER, Helbling Lichtenhahn, 2. Auflage 2014, Basel ad Art. 274, S. 2168, RZ 4 in fine; SYLVAIN MÉTILLE, op.cit. ad Art. 274, S. 1796, RZ 23 («Le délai [de vingt-quatre heures] se compte à la minute près, dès la transmission de l'ordre de surveillance au Service SCPT»)

12 Namentlich DANIEL STOLL, in KUHN/ JEANNERET, Commentaire romand du Code de procédure pénale suisse, Helbling Lichtenhahn, 2. Auflage 2019, Basel, ad Art. 90, S. 430 und 431, RZ 12

13 Insbesondere BGE 144 IV 161 (Urteil 6B_80/2018 vom 25.04.2018)

14 S. auch z. B. Art. 22 Abs. 2 der Verordnung vom 30.08.1995 über die Wehrpflichtersatzabgabe (**WPEV**; SR **661.1**)

am 31. des Monats durch den Dienst ÜPF empfangen wird, dann ist der Tag des frühestmöglichen Beginns der rückwirkenden Überwachung auch der 31. des entsprechenden Monats 6 Monate früher. Wenn es aber den 31. im Monat des Beginns der Überwachung nicht gibt (z. B. keinen 31. April), dann nimmt man den letzten existierenden Tag dieses Monats (30. April, s. unten die Beispiele 2 und 3).

Nach *Absatz 2* endet eine rückwirkende Überwachung standardmässig spätestens am Tag des Empfangs der Anordnung durch den Dienst ÜPF, das heisst spätestens um 23.59 Uhr und 59 Sekunden[15] Schweizer Zeit dieses Tages (s. u. Bsp. 1-4). Normalerweise werden rückwirkende Überwachungen erst an einem der Folgetage ausgeführt (Bearbeitungsfrist im Normalfall 3 Arbeitstage). Wird die rückwirkende Überwachung jedoch noch am selben Tag - also noch vor 23.59 Uhr und 59 Sekunden – ausgeführt, so bekommt die berechtigte Behörde nur die bis zum Zeitpunkt der Ausführung bei der Anbieterin vorhandenen Randdaten (Historische Daten, HD). Es erfolgt somit keine zweite nachträgliche Datenlieferung der restlichen HD, die zwischen dem Zeitpunkt der Ausführung der Überwachung und dem Ende dieses Tages anfallen. Dies ist insbesondere dann relevant, wenn eine rückwirkende Überwachung für dringend erklärt worden ist (s. Bsp. 5). Wenn relevante HD bei der Anbieterin aufgrund von üblichen Verzögerungen erst später verfügbar sind (beispielsweise Daten aus dem Roaming), müssen diese ebenfalls nicht nachgeliefert werden. Falls diese HD für die anordnende Behörde von Wichtigkeit sind, sollte sie eine weitere rückwirkende Überwachung zu einem späteren Zeitpunkt in Erwägung ziehen (s. auch unten Bsp. 5). Ein Anspruch auf Nachlieferung von aus objektiven Gründen zum Zeitpunkt der Lieferung noch nicht bei der Anbieterin vorhandenen HD wäre hier mit einem unverhältnismässigen Aufwand bei den Anbieterinnen verbunden. Die anordnende Behörde kann den Ausführungszeitpunkt der rückwirkenden Überwachung entsprechend steuern, je nachdem welche HD für sie wichtig sind (die ältesten oder die jüngsten). Wenn die ältesten HD wichtig sind, muss die Anordnung der rückwirkenden Überwachung so rasch wie möglich erfolgen. Um die jüngsten HD vollständig zu bekommen, hat die anordnende Behörde die Wahl zwischen zwei Varianten: entweder eine normale Anordnung einer HD-Überwachung mit Ausführung an einem der Folgetage, falls die HD nicht sofort benötigt werden, oder eine Anordnung einer Echtzeitüberwachung «nur Randdaten (IRI only)», falls die jüngsten Randdaten sofort benötigt werden und die unvermeidliche Verzögerung bei HD vermieden werden soll. Historische Randdaten (HD) und Echtzeitranddaten (IRI) sind jedoch in Umfang und Detaillierung nicht identisch. In der Regel sind IRI umfangreicher und detaillierter.

Die zur Aufbewahrung von Randdaten verpflichteten Anbieterinnen müssen sicherstellen, dass sie die Randdaten lange genug aufbewahren. Dabei haben sie die vorgenannte Regel zur Berechnung des frühestmöglichen Beginns einer rückwirkenden Überwachung sowie die Bearbeitungsfristen nach den Artikeln 17 und 18 VD-ÜPF zu berücksichtigen. Die Anbieterin führt die rückwirkende Überwachung im Normalfall innerhalb von 3 Arbeitstagen aus, bei dringenden Fällen innerhalb von 6 Stunden (Art. 17 Abs. 3 VD-ÜPF).

[15] Bei rückwirkenden Überwachungen wird die Zeit auf die Sekunde genau angegeben, d.h. auf volle Sekunden gerundet.

Im Folgenden werden einige Beispiele für die Berechnung der Frist von 6 Monaten aufgeführt. Dabei gibt es anzumerken, dass die Uhrzeit (Schweizer Zeit) des Beginns der Überwachung standardmässig 00.00 Uhr und 0 Sekunden[16], und die Uhrzeit des Endes der Überwachung standardmässig 23.59 Uhr und 59 Sekunden ist (in den Beispielen werden die Sekunden nicht angegeben). Eine Ausnahme besteht, wenn die Ausführung noch am Tag der Anordnung stattfindet. Dann ist die Uhrzeit des Endes gleich der minutengenauen Uhrzeit der Ausführung plus 59 Sekunden. Die Anbieterin hat die im Moment der Ausführung vorhandenen HD zu liefern.

Beispiel 1: Anordnung, die auf Dienstag, 08.11.2022, datiert ist, wird aufgrund interner Verzögerungen bei der anordnenden Behörde erst am Donnerstag, **10.11.2022,** um 9.00 Uhr mittels verschlüsseltem Mail verschickt und vom Dienst ÜPF zeitgleich empfangen.
→ Beginn Tag **TT = 10**, Monat MM: 11 - 6 = 5 → **MM = 5**, Jahr **JJJJ = 2022**
Frühestmöglicher Beginn ist der 10.05.2022, 00.00 Uhr;
spätestmögliches Ende ist der 10.11.2022, 23.59 Uhr.

Bemerkung: Dieses Beispiel illustriert das Problem der verzögerten Übermittlung der Anordnung. Die anordnende Behörde hätte bei sofortiger Übermittlung die HD ab dem 08.05.2022 bekommen können, also 2 Tage früher. Jedoch wäre dann auch das Ende der Überwachung 2 Tage früher auf den 08.11.2022 gefallen.

Beispiel 2: Anordnung hochgeladen in WMC am Mittwoch, **31.08.2022,** um 18.00 Uhr
→ Beginn **TT = 31**, MM: 8 – 6 = 2 → **MM = 02**, **JJJJ = 2022.**
Den 31.02.2022 gibt es nicht, also wird auf den letzten Tag des Februars in 2022 «abgerundet».
Frühestmöglicher Beginn ist der 28.02.2022, 00.00 Uhr;
spätestmögliches Ende ist der 31.08.2022, 23.59 Uhr.

Beispiel 3: Mündliche Anordnung per Telefon an den Dienst ÜPF am Sonntag, **31.12.2023,** um 16.50 Uhr.
→ Beginn **TT = 31**, MM: 12 - 6 = 6 → **MM** = **06**, **JJJJ = 2023**
Den 31.06.2023 gibt es nicht, also wird auf den letzten Tag des Juni «abgerundet».
Frühestmöglicher Beginn ist der 30.06.2023, 00.00 Uhr;
spätestmögliches Ende ist der 31.12.2023, 23.59 Uhr.

Beispiel 4: Anordnung datiert vom Mittwoch, 13.04.2022, per Post am Donnerstag, 14.04.2022, (Poststempel) geschickt, keine telefonische Avisierung. Im Dienst ÜPF am Dienstag (nach Ostermontag), **19.04.2022**, um 9.00 Uhr erhalten. Überwachungsauftrag am 19.04.2022 um 9.50 Uhr an die Anbieterin weitergeleitet.
→ Beginn **TT = 19**, MM: 4 - 6 = -2 + 12 → **MM** = **10** des Vorjahres, JJJJ: 2022 - 1 → **JJJJ = 2021**
Frühestmöglicher Beginn ist der 19.10.2021, 00.00 Uhr;
spätestmögliches Ende ist der 19.04.2022, 23.59 Uhr.

16 Bei rückwirkenden Überwachungen wird die Zeit auf die Sekunde genau angegeben, d.h. auf volle Sekunden gerundet.

Bemerkung: Bei telefonischer Anordnung gilt der Tag des Anrufs als Stichtag, nicht der Tag des Empfangs der schriftlichen Bestätigung (s. Bsp. 3). Im vorliegenden Beispiel hätte bei telefonischer Avisierung am 14.04.2022 (5 Tage früher) die rückwirkende Überwachung bereits am 14.10.2021 beginnen können, hätte dementsprechend aber auch spätestens am 14.04.2022 geendet.

Beispiel 5: Anordnung einer **dringenden** rückwirkenden Überwachung, hochgeladen im WMC durch die anordnende Behörde am Freitag, **26.08.2022**, **um 16.00 Uhr**, beauftragt an die MWP durch den Dienst ÜPF um 16.30 Uhr.
→ Beginn **TT = 26**, MM: 8 - 6 = 2 → **MM = 02**, **JJJJ = 2022**
Frühestmöglicher Beginn ist der 26.02.2022, 00.00 Uhr;
spätestmögliches Ende ist der 26.08.2022.

Da das Ende der rückwirkenden Überwachung auf den Ausführungstag fällt, bestimmt sich die für das Ende massgebliche Uhrzeit hier aus dem Zeitpunkt der Ausführung durch die MWP (sie hat max. 6 h Zeit nach Erhalt des Auftrags, d. h. spätestens bis 22:30 Uhr). Aus technischen Gründen können gerade erst angefallene HD bei der MWP noch nicht zur Lieferung bereitstehen. Hierbei hat die anordnende Behörde zwischen der Schnelligkeit der Lieferung und der Verfügbarkeit der Randdaten abzuwägen. Rückwirkende Randdaten können bei der MWP erst mit einigen Stunden Verzögerung verfügbar sein. Es sollte eine rückwirkende Überwachung zu einem späteren Zeitpunkt (Achtung: Verlust der ältesten Randdaten beachten) oder, bei zeitkritischen Überwachungen, eine Echtzeitüberwachung «nur Randdaten» in Erwägung gezogen werden (s. oben).

Art. 11 Leistungen ausserhalb der Normalarbeitszeiten und an Feiertagen

Diese Bestimmung wird aufgrund der zahlreichen Änderungen in ihrer Gesamtheit revidiert. Sie regelt die Leistungen des Dienstes ÜPF sowie der genannten MWP ausserhalb der Normalarbeitszeiten, das heisst Montag bis Freitag zwischen 17.01 Uhr und 7.59 Uhr und ganztägig an Wochenenden sowie Feiertagen (s. Art. 10). Während dieser Zeit wird durch den Dienst ÜPF und die genannten MWP ein Pikettdienst zur Verfügung gestellt. Die Bearbeitungsfristen für die Leistungen des Dienstes ÜPF sowie der MWP während des Pikettdienstes sind, wie auch jene während der Normalarbeitszeiten, in der VD-ÜPF geregelt. Leistungen für standardisierte Auskünfte (Art. 26 Abs. 1) und standardisierte Überwachungen (Art. 28), die für eine MWP nicht Teil ihrer Pikettpflichten sind, dürfen von der MWP freiwillig im Pikett erbracht werden, wobei sie nicht den Bearbeitungsfristen unterliegt.

Absatz 1 wird angepasst und neu strukturiert. Materiell gibt es kaum Änderungen für den Dienst ÜPF, die Behörden und die MWP. Insbesondere ist für die MWP die Störungsbehebung schon in der bisherigen Fassung von Artikel 11 vorhanden (Abs. 1 Bst. e i. V. m. Abs. 2) sowie auch die Erreichbarkeit während 24 Stunden am Tag und 7 Tagen die Woche («jederzeit» in Abs. 2 in fine). Die FDA mit vollen Pflichten (d.h. die nicht nach Artikel 51 befreit sind) und die AAKD mit weitergehenden Überwachungspflichten (Art. 52) haben alle Pikettleistungen nach Absatz 1 Buchstaben a–e zu erbringen, soweit sie dazu gemäss den Artikeln 18 und 50 verpflichtet sind. Diese Einschränkung erfolgt, da AAKD mit weitergehenden Überwachungspflichten (Art. 52) die neuen Auskünfte gemäss den Artikeln 48*a*–48*c* nicht erteilen und die

neuen Überwachungen gemäss Artikel 56*a* und 56*b* sowie die entsprechenden neuen Notsuchen gemäss Artikel 67 Buchstaben b und c und die entsprechenden neuen Fahndungen gemäss Artikel 68 Absatz 1 Buchstaben b und c nicht durchführen müssen. Nicht in diesem Absatz erwähnt werden die FDA mit reduzierten Überwachungspflichten (Art. 51), die AAKD ohne weitergehende Pflichten (d. h. diejenigen, die die Voraussetzungen von Art. 22 und 52 nicht erfüllen), die AAKD mit weitergehenden Auskunftspflichten (Art. 22) sowie die MWP nach Artikel 1 Absatz 2 Buchstaben k, l und m, da sie keinen Pikettdienst leisten müssen.

In den Buchstaben a–e werden die Leistungen im Pikettdienst abschliessend aufgeführt. Zu beachten ist, dass der Dienst ÜPF im Pikettdienst nur eine eingeschränkte Beratung leistet. In *Buchstabe a* ist die Erteilung gewisser Auskünfte geregelt. Festzuhalten ist, dass Auskünfte gemäss den Artikeln 44–48 während dem Pikettdienst nicht zwingend erbracht werden müssen. In *Buchstabe b* ist geregelt, welche Typen von Echtzeitüberwachungen im Pikett aktiviert werden. In *Buchstabe c* ist festgelegt, welche Typen von als dringend erklärten rückwirkenden Überwachungen im Pikett durchgeführt werden. In *Buchstabe d* sind die Typen von Notsuchen und Fahndungen aufgeführt, die im Pikett durchgeführt werden. Der seit 1. Juni 2022 in Kraft getretene Buchstabe d[bis][17] wird zum neuen *Buchstaben e*.

In *Absatz 2* wird die aktuelle Praxis verankert, wonach die Behörden alle Aufträge im Pikettdienst telefonisch über die Pikettnummer des Dienstes ÜPF avisieren müssen. Davon ausgenommen sind lediglich die automatisiert erteilten Auskünfte. Nur so kann sichergestellt werden, dass die Mitarbeitenden des Dienstes ÜPF rechtzeitig auf die Aufträge aufmerksam werden und sie fristgerecht bearbeiten sowie ihrerseits die betreffende MWP über den Auftrag informieren können.

Absatz 3 bleibt im Vergleich zum bisherigen Absatz 3 materiell unverändert. Es wird lediglich eine redaktionelle Änderung vorgenommen, um den gleichen Wortlaut wie in Absatz 1 zu verwenden («ausserhalb der Normalarbeitszeiten und an Feiertagen»). Absatz 3 besagt, dass die besonderen Auskünfte und Überwachungen (sog. Spezialfälle gemäss Art. 25) von den Pikettdienstleistungen ausgenommen sind. Dabei handelt es sich um Auskünfte beziehungsweise Überwachungen, die keinem Auskunftsbeziehungsweise Überwachungstyp der Verordnung entsprechen (sog. nicht-standardisierte Auskünfte bzw. -Überwachungen) und vom Dienst ÜPF oder durch von diesem beauftragte Personen durchgeführt werden. Die Erteilung dieser Auskünfte beziehungsweise die Durchführung dieser Überwachungen sind erheblich komplexer als standardisierte Typen. Sie sind nicht planbar und der Personalaufwand ist nur schwer abschätzbar. Es wäre mit unverhältnismässig hohen Kosten verbunden, das erforderliche Personal im Pikett beim Dienst ÜPF oder dessen Beauftragten bereitzuhalten.

Absatz 4 sieht neu vor, dass MWP, die keinen Pikettdienst nach Absatz 1 leisten müssen, jedoch aus anderweitigen Gründen ausserhalb der Normalarbeitszeit und an Feiertagen erreichbar sind, die entsprechenden Kontaktnummern beziehungsweise Kontaktpersonen dem Dienst ÜPF mitzuteilen haben. Die MWP erhalten diesbezüglich keine neuen Verpflichtungen, insbesondere sollen sie nicht verpflichtet werden, einen Pikettdienst speziell für den Dienst ÜPF einzurichten. Wenn aber bereits ein solcher

[17] Verordnung vom 04.05.2022 über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (**VPMT**; AS **2022** 301)

besteht, sollen die allfällig vorhandenen Kontaktangaben dem Dienst ÜPF mitgeteilt werden. Selbst wenn es sich bei diesen Kontakten nicht um Spezialisten aus dem Bereich der Überwachung handelt (sogenannte «LI-Officer»), werden sie dem Dienst ÜPF bei besonders dringenden Fällen ausserhalb der Normalarbeitszeiten und an Feiertagen weiterhelfen können. «Besonders dringende Fälle» sind zum Beispiel Bombendrohungen, Entführungen oder andere Fälle, in denen das Leben oder die körperliche Integrität von Personen auf dem Spiel steht. In solchen Fällen würden der Dienst ÜPF oder die Polizeibehörden versuchen, irgendeine Person bei der MWP zu erreichen. Die Angabe einer Kontaktnummer oder Kontaktperson vereinfacht somit die Aufgaben des Dienstes ÜPF, der Strafverfolgungsbehörden und der MWP.

Art. 18 Pflichten für die Lieferung von Auskünften durch FDA und AAKD mit weitergehenden Pflichten

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert. Der bisherige Artikel 18 wird für die bessere Lesbarkeit neu in vier Artikel (Art. 18, 18*a*, 18*b* und 18*c*) aufgeteilt. In diesen Artikeln werden die Pflichten im Zusammenhang mit der Auskunftserteilung näher bestimmt.

Artikel 18 Absatz 1 legt den Grundsatz fest, wonach die FDA mit vollen Pflichten sowie die AAKD mit weitergehenden Pflichten (Art. 22 oder Art. 52) die Auskünfte über die IRC[18] zu erteilen haben.

Die bisherigen Absätze 1 und 4 sahen vor, dass die MWP die Auskünfte erteilen müssen, die durch sie angebotene Dienste betreffen. Der Zusatz «die durch sie angebotene Dienste betreffen» wird in der aktuellen Fassung nicht übernommen, da er redundant ist. Die Pflicht zur Erteilung von Auskünften umfasst weiterhin nur die von den MWP angebotenen Dienste.

In *Absatz 2 erster Satz* wird geregelt, welche Auskunftstypen von den FDA mit vollen Pflichten automatisiert zu beantworten sind. Die Pflicht zur Automatisierung betrifft häufige, zeitkritische oder einfach zu beantwortende Auskünfte. Der *zweite Satz* präzisiert, dass die vorerwähnten FDA bei den übrigen standardisierten Auskünften (die übrigen Auskunftstypen der VÜPF) die Wahl zwischen manueller und, im Einvernehmen mit dem Dienst ÜPF, automatisierter Erteilung haben.

Die Wahlmöglichkeit zwischen automatisierter und manueller Auskunftserteilung besteht auch für andere MWP (s. Abs. 3 und 4). Sie ist im Sinne der wirtschaftlichen Freiheit der betroffenen MWP zu sehen, da die Automatisierung von Auskünften Investitionskosten verursacht, dadurch andererseits aber auch operationelle Kosten im Vergleich zur manuellen Erteilung eingespart werden können. Der Dienst ÜPF entscheidet im Einvernehmen mit der MWP, ob die jeweilige Automatisierung für den gewünschten Auskunftstyp in der IRC umgesetzt werden kann. Diese Wahlmöglichkeit führt dazu, dass einige MWP Auskünfte eines bestimmten Typs manuell erteilen, während andere MWP die Auskünfte des gleichen Typs automatisiert beantworten. Änderungen an automatisierten Auskunftstypen verursachen bei den betroffenen

18 Information Request Component (IRC); Komponente zur Erteilung von Auskünften des Verarbeitungssystems des Dienstes ÜPF (s. das Programm FMÜ); in Betrieb seit dem 18.03.2019.

MWP unter anderem Aufwendungen für entsprechende Anpassungen an ihren Kundenmanagement- und anderen Systemen, um die geforderten Informationen automatisiert liefern zu können. Bei solchen Änderungen müssen daher auch die Aspekte der Verhältnismässigkeit im Auge behalten werden, ob beispielsweise die Häufigkeit der Nutzung des entsprechenden Auskunftstyps eine Automatisierung weiterhin rechtfertigt. Aus diesem Grund wird der weniger häufig gebrauchte Auskunftstyp gemäss Artikel 42 (IR_13_EMAIL) neu nicht mehr der Gruppe der «zwingend automatisierten» Auskünfte (vgl. bisherigen Abs. 2) zugeteilt, sondern den «anderen Auskünften», bei welchen auch für die MWP mit vollen Pflichten die Wahl zwischen manueller und, im Einvernehmen mit dem Dienst ÜPF, automatisierter Erteilung besteht.

Von den drei neuen Auskunftstypen muss nur der Auskunftstyp gemäss Artikel 48*b* (IR_52_ASSOC_TEMP) von den betroffenen FDA automatisiert erteilt werden, weil bei diesem Typ eine manuelle Erteilung unmöglich ist, da die Daten unmittelbar zur Verfügung stehen müssen. Bei den beiden anderen neuen Auskunftstypen gemäss Artikel 48*a* (IR_51_ASSOC_PERM) und gemäss Artikel 48*c* (IR_53_TEL_ADJ_NET) haben die betroffenen FDA die Wahl zwischen manueller und, im Einvernehmen mit dem Dienst ÜPF, automatisierter Erteilung.

Die automatisierte und die manuelle Auskunftserteilung über die IRC können wie folgt unterschieden werden: Die automatisierte Auskunftserteilung läuft ohne menschliche Mitwirkung des Dienstes ÜPF und der MWP ab; die berechtigte Behörde gibt ihr Auskunftsgesuch in die IRC ein und erhält spätestens innert 1 Stunde die Antwort von den Systemen der MWP. Bei der manuellen Erteilung der Auskunft über die IRC gibt die berechtigte Behörde ihr Auskunftsgesuch in die IRC ein und die MWP erhält eine Mitteilung, dass ein Auskunftsgesuch für sie eingetroffen ist. Die Mitarbeitenden der MWP melden sich in der IRC an und füllen dort von Hand die entsprechende Antwortmaske aus. Die berechtigte Behörde erhält die Antwort ebenfalls in der IRC.

Als dritte Möglichkeit gibt es die manuelle Erteilung der Auskunft ausserhalb des Verarbeitungssystems (Abs. 3 Bst. a). Dabei gibt die berechtigte Behörde ihr Auskunftsgesuch in die IRC ein, der Dienst ÜPF übermittelt dieses jedoch ausserhalb der IRC über ein vom EJPD zugelassenes schriftliches Übertragungsmittel an die MWP. Die MWP kann die Auskunft formlos erteilen und übermittelt die Antwort über ein vom EJPD zugelassenes schriftliches Übertragungsmittel an den Dienst ÜPF. Dieser übermittelt die Antwort gesichert an die berechtigte Behörde.

Absatz 3 regelt die Auskunftserteilung der FDA mit reduzierten Überwachungspflichten (Art. 51). Sie sind von der Auskunftserteilung nach Artikel 48*b* aufgrund der Verhältnismässigkeit befreit. Die Auskunftserteilung nach Artikel 48*b* erfordert aufgrund des zeitkritischen Ablaufs eine aktive Vorbereitung der betroffenen FDA, welche mit der Ausführung von Echtzeitüberwachungen und damit mit den Überwachungspflichten gemäss Artikel 26 BÜPF vergleichbar ist. Die Umsetzung dieses echtzeitnah zu beantwortenden Auskunftstyps erfordert insbesondere Investitionen der betroffenen FDA in eine neue Anfrageschnittstelle und in das System zur automatisierten Auskunftserteilung. Diese Zusatzbelastungen sollen nur den grossen FDA auferlegt werden. Im Gegensatz zu den übrigen Auskünften besteht bei dem Auskunftstyp nach

Artikel 48*b* die Besonderheit, dass eine manuelle Auskunftserteilung oder die Lieferung der ihr vorliegenden Angaben durch die betroffene FDA ohne aktive Vorbereitung kaum praktikabel ist.

Für die Erteilung der übrigen standardisierten Auskünfte (Art. 26 Abs. 1) gilt für FDA mit reduzierten Überwachungspflichten die Mindestanforderung gemäss *Buchstabe a*: die manuelle schriftliche Auskunftserteilung ausserhalb des Verarbeitungssystems. Es besteht für sie jedoch auch die freiwillige Möglichkeit der manuellen Auskunftserteilung über die IRC (*Bst. b*, s. Erläuterungen zu Abs. 2). Eine FDA mit reduzierten Überwachungspflichten kann den Wunsch äussern, bestimmte Auskünfte automatisiert zu erteilen (*Bst. c*). Der Dienst ÜPF entscheidet dann im Einvernehmen mit ihr, ob dies in der IRC umgesetzt werden kann.

In *Absatz 4 erster Satz* wird geregelt, welche Auskunftstypen von den AAKD mit weitergehenden Pflichten (Art. 22 oder Art. 52) automatisiert zu beantworten sind. Der *zweite Satz* sieht vor, dass die vorgenannten AAKD von der Auskunftserteilung nach den neuen Artikeln 48*a*-48*c* befreit sind. Ob diese Auskünfte zukünftig gegebenenfalls auch durch die AAKD erteilt werden müssen, wird im Rahmen der zweiten Revision entschieden, wenn die nähere Umschreibung der Kategorien FDA und AAKD umgesetzt wird. Es wird daher vorliegend davon abgesehen, den AAKD neue Pflichten im Zusammenhang mit diesen neuen Auskunftstypen aufzuerlegen. Der *dritte Satz* enthält die zu Absatz 2 zweiter Satz (s. die dortigen Erläuterungen) analoge Regelung zur Wahlmöglichkeit zwischen der automatisierten und der manuellen Auskunftserteilung über die IRC.

Art. 18a Pflichten für die Lieferung von Auskünften durch die AAKD ohne weitergehende Pflichten und die Betreiberinnen von internen Fernmeldenetzen

Der zur besseren Lesbarkeit neu eingefügte Artikel 18a regelt die Pflichten für die Lieferung von Auskünften durch die AAKD ohne weitergehende Pflichten, das heisst AAKD, die weder weitergehende Auskunftspflichten (Art. 22) noch weitergehende Überwachungspflichten (Art. 52) haben, und die Betreiberinnen von internen Fernmeldenetzen.

Absatz 1 führt aus, dass sie sich bei der Auskunftserteilung nicht an die in dieser Verordnung vorgesehenen Typen zu halten haben. Da sie keine Auskunftsbereitschaft sicherstellen müssen, müssen sie lediglich die Angaben liefern, die ihnen vorliegen.

Absatz 2 regelt die Frage der Lieferung der Angaben. Als Mindestanforderung liefern die AAKD ohne weitergehende Pflichten und die Betreiberinnen von internen Fernmeldenetzen die ihnen vorliegenden Angaben schriftlich ausserhalb des Verarbeitungssystems mittels eines durch das EJPD zugelassenen sicheren Übertragungsmittels.

Gemäss *Absatz 3* haben sie jedoch auch die Möglichkeit, die ihnen vorliegenden Angaben über die Abfrageschnittstelle (IRC) des Verarbeitungssystems manuell oder, im Einvernehmen mit dem Dienst ÜPF, automatisiert zu liefern.

Art. 18b Beizug Dritter bei der Auskunftserteilung

Im zur besseren Lesbarkeit neu eingefügten Artikel 18*b* wird die Regelung des bisherigen Artikels 18 Absatz 1 zweiter Satz und Absatz 4 zweiter Satz übernommen. Danach können die MWP Dritte zur Auskunftserteilung beiziehen.

Art. 18c Bekanntgabe der Anzahl Datensätze bei der Auskunftserteilung

Auch dieser Artikel wurde zur besseren Lesbarkeit neu eingefügt und enthält die Regelung des bisherigen Artikels 18 Absatz 6.

Art. 20 Überprüfung der Angaben zur Person bei Mobilfunkdiensten

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert. Bei Mobilfunkdiensten bestehen strengere Vorgaben zur Identifikation als bei anderen Diensten, wie WLAN (vgl. Art. 19). Diese Bestimmung, wie auch die Artikel 20*a* und 20*b*, stützt sich namentlich auf die Delegationsnormen an den Bundesrat in Artikel 21 Absatz 1 Buchstabe d, Artikel 22 Absatz 2 und Artikel 23 Absatz 1 BÜPF. Die unterschiedlichen Bestimmungen bei natürlichen (Art. 20*a*) und juristischen Personen (Art. 20*b*) werden ergänzt und klarer dargestellt.

Absatz 1 legt den Grundsatz fest. Bei der Abgabe der Zugangsmittel zu Mobilfunkdiensten (z. B. GSM, GPRS, UMTS, LTE, VoLTE, VoWiFi, 5G) oder, falls diese erst durch Aktivierung für die Teilnehmende nutzbar werden, bei der erstmaligen Aktivierung dieser Dienste, müssen die FDA respektive die Wiederverkäuferinnen (Abs. 2) bei natürlichen Personen die Identität der oder des Teilnehmenden (Art. 20*a*) und bei juristischen Personen deren Angaben (Art. 20*b*) überprüfen.

Unter Aktivierung beziehungsweise Freischaltung ist der Zeitpunkt zu verstehen, ab dem die Teilnehmenden den entsprechenden Dienst nutzen können. Bei bereits sofort nutzbaren Zugangsmitteln ist dies beispielsweise der Zeitpunkt deren Abgabe. Bei einer fest im Gerät eingebauten SIM (Embedded SIM; eSIM) wird in der Regel das entsprechende Profil durch die Anbieterin aktiviert. Sie kann den Dienst auch durch die Aufhebung einer allfälligen Blockierung freischalten. Wenn zum Beispiel ein für Mobilfunk vorbereitetes Tablet mit eSIM von einem Elektronikgeschäft an eine Kundin oder einen Kunden verkauft wird, kann diese oder dieser das Tablet zunächst nicht für den mobilen Internetzugang benutzen, solange die eSIM nicht aktiviert beziehungsweise freigeschaltet ist. Erst wenn die Kundin oder der Kunde sie von einer Mobilfunkanbieterin aktivieren lässt, kann sie oder er dieses Zugangsmittel zum Mobilfunknetz benutzen. Das Zugangsmittel ist fest im Tablet eingebaut und wird schon beim Verkauf des Tablets «abgegeben». Da es zu diesem Zeitpunkt aber noch nicht funktionieren kann, interessiert die Strafverfolgungsbehörden erst der Moment, wenn es aktiviert und damit im Mobilfunknetz nutzbar wird. Ausserdem ist wichtig, wer die Identifizierung der oder des Teilnehmenden und die Registrierung der Angaben zur Person durchführen muss. Das Elektronikgeschäft führt in diesem Beispiel die Aktivierung des Zugangsmittels zum Mobilfunk nicht durch. Daher muss das Elektronikgeschäft hier auch nicht registrieren, das heisst es gilt in diesem Beispiel nicht als professionelle Wiederverkäuferin von Karten und ähnlichen Mitteln (Art. 2 Bst. f BÜPF). Dies ist Aufgabe der Mobilfunkanbieterin in ihrer Eigenschaft als FDA bei

der Übertragung des Profils auf die eSIM (virtuelle SIM-Karte als Zugangsmittel zum Mobilfunknetz) und anschliessenden Aktivierung des Profils auf der eSIM.

Absatz 2 stellt klar, dass die Überprüfung der Identität der oder des Teilnehmenden (Art. 20*a*) respektive die Überprüfung der Angaben der juristischen Person (Art. 20*b*) durch die professionellen Wiederverkäuferinnen (Art. 2 Bst. f BÜPF) vorzunehmen ist, falls die Abgabe des Zugangsmittels oder die erstmalige Aktivierung unmittelbar durch diese erfolgt. So wird zum Beispiel bei der Abgabe des Zugangsmittels in einem Shop die Identifizierung der oder des Teilnehmenden von einer professionellen Wiederverkäuferin vorgenommen. Dabei kopiert sie das jeweilige Identifizierungsmittel (z. B. den Ausweis) und übermittelt dann die vorgeschriebenen Angaben zur Person und die elektronische Kopie des Identifizierungsmittels gemäss Artikel 20*a* Absatz 4 an die FDA.

Absatz 3 sieht vor, dass die ordnungsgemässe Registrierung und Identifizierung der oder des Teilnehmenden durch die professionelle Wiederverkäuferin sowie die Weiterleitung der Angaben und der Ausweiskopie an die FDA durch die FDA in geeigneter Weise zu überprüfenist. Die FDA muss letztlich in der Lage sein, die geforderten Auskünfte erteilen zu können und kann sich nicht auf Versäumnisse der professionellen Wiederverkäuferin berufen.

Bei erneuten Kundenkontakten im Verlaufe der Kundenbeziehung kann davon ausgegangen werden, dass die FDA in der Regel auch deren Angaben aktualisieren und diese gegebenenfalls prüfen, weil sie ein eigenes Interesse daran haben. Wenn sich zum Beispiel die Adresse einer Kundin oder eines Kunden ändert und die FDA darüber informiert wird, speichert die FDA diese Adressänderung in ihrer Kundendatenbank ab. Bei einem allfälligen Auskunftsgesuch sind neben den vorgeschriebenen Kundendaten auch alle weiteren vorhandenen Kontaktdaten (z. B. geänderte Adressen) und jeweils deren Gültigkeitszeitraum zu liefern. Es besteht jedoch keine Pflicht zur fortlaufenden Überprüfung und lückenlosen Aktualisierung dieser Daten. So wird insbesondere auch keine Nachregistrierung von zwischenzeitlich geänderten Angaben zur Person verlangt. Wenn eine FDA Kenntnis von einer Änderung von Kundendaten erlangt, hat sie diese im Rahmen einer allfälligen Auskunft auch entsprechend mitzuteilen.

Art. 20a Erbringung des Identitätsnachweises bei natürlichen Personen bei Mobilfunkdiensten

In *Absatz 1* werden die zugelassenen Identifikationsmittel für den Identitätsnachweis abschliessend genannt. Andere Mittel wie ein Führerausweis sind nicht zugelassen. Beim Reisepass (*Bst. a*) und bei der Identitätskarte (*Bst b*) kann es sich sowohl um ein schweizerisches wie auch um ein ausländisches Dokument handeln. Die Überprüfung der Identität der Kundin oder des Kunden mittels eines der genannten Identifikationsmittel ist für Mobilfunkdienste zwingend. Dies entspricht der früheren Regelung für vorbezahlte Mobilfunkdienste (Prepaid), welche mit der totalrevidierten VÜPF auf

alle Mobilfunkdienste unabhängig von der Zahlungsmethode (z. B. Abonnement, vorbezahlt, gratis) ausgedehnt wurde[19]. In der Praxis verlangen die Mobilfunkanbieterinnen beim Abschluss von Abonnementen bereits seit langem die Vorlage eines Ausweisdokuments. Das Ausweisdokument muss von der Anbieterin respektive professionellen Wiederverkäuferin nicht minuziös auf seine Echtheit hin überprüft werden. Hierzu ist sie faktisch auch nicht in der Lage, denn ihr stehen nicht die gleichen Prüfungsmöglichkeiten wie etwa einer polizeilichen Behörde zur Verfügung. Die Anbieterin respektive professionelle Wiederverkäuferin ist jedoch dazu angehalten, das Ausweisdokument nur dann zu akzeptieren, wenn es plausibel scheint, dass das Dokument echt ist. Akzeptiert eine Anbieterin respektive professionelle Wiederverkäuferin ein Ausweisdokument, das offensichtlich als Fälschung erkannt werden kann oder offensichtlich nicht zu der Person passt, die es vorgelegt hat, hat dies für die Anbieterin respektive professionelle Wiederverkäuferin unter Umständen verwaltungsstrafrechtliche Folgen (vgl. Art. 39 BÜPF).

Buchstaben a-c entsprechen den zugelassenen Ausweisdokumenten im geltenden Artikel 20 Absatz 1. Will sich die Kundin oder der Kunde beim Mobilfunkdienst mit einem dieser Dokumente identifizieren lassen, wird sie oder er sich in der Regel damit vor Ort ausweisen. Da der Vorgang des Identitätsnachweises nicht vorgeschrieben ist, ist auch eine Video- oder Online-Identifizierung möglich[20]. In diesem Fall sind die Sicherheits- und Qualitätsstandards des FINMA-Rundschreibens 2016/7 «Video- und Online-Identifizierung»[21] für die Onlineidentifizierung im Bankenbereich einzuhalten.

Das Ausweisdokument (Bst. a-c) muss am Erfassungstag gültig sein. Für den Erfassungstag wird auf den Zeitpunkt abgestellt, wenn die Kundin oder der Kunde für ihre oder seine Identifikation der Anbieterin respektive der professionellen Wiederverkäuferin ihren oder seinen Ausweis vorlegt. Nur mit einem gültigen Ausweis kann die sichere Identifikation gewährleistet werden. Die Praxis zeigt, dass mit abgelaufenen Ausweisdokumenten in der Vergangenheit Falschregistrierungen vorgenommen wurden.

Die in *Absatz 2* genannten Angaben entsprechen denjenigen im geltenden Artikel 20 Absatz 2. Sie stützen sich auf Artikel 21 Absatz 1 BÜPF. Die FDA beziehungsweise die professionelle Wiederverkäuferin muss dafür sorgen, dass die Erfassung der Angaben zur Person korrekt anhand des vorgezeigten Identifizierungsmittels erfolgt. Zur Kontrolle dient bei physischen Ausweisen die Kopie des vorgezeigten Identifizierungsmittels. Falls das Identifizierungsmittel (z. B. Ausweis) über eine maschinenlesbare Zone (MRZ) verfügt, wird empfohlen, die Angaben in der MRZ maschinell auszulesen und wie folgt zu erfassen:

- Name(n) und Vorname(n) aus der MRZ als Alias beziehungsweise Nebenidentität. Da diese im reduzierten lateinischen Zeichensatz vorliegen

19 Gemäss Urteil des EGMR vom 30.01.2020 (Az. 50001/12) i.S. Breyer gegen Deutschland verletzt die Identifizierungspflicht bei Prepaid-SIM-Kauf die Privatsphäre gemäss Art. 8 EMRK nicht.

20 Vgl. auch Art. 6 Abs. 4 Bst. b Geldwäschereiverordnung EJPD **(GwV-EJPD;** SR **955.022)** und Art. 5 Abs. 1 Bst. e Geldwäschereiverordnung ESBK (**GwV-ESBK**; SR **955.021**)

21 finma.ch =>Dokumentation => Rundschreiben

(Transliteration), können sie direkt für die normale, das heisst buchstabengetreue, Namenssuche verwendet werden (s. Art. 35).

Für die folgenden Angaben zur Person beziehungsweise zum Ausweis sollten, falls vorhanden, die MRZ-Daten erfasst werden, statt einer manuellen Eingabe:

- Ausstellendes Land beziehungsweise Organisation (dreibuchstabige Abkürzung);
- Ausweisnummer;
- Nationalität (dreibuchstabige Abkürzung);
- Geburtsdatum (YYYYMMDD);
- Geschlecht (M=männlich / F=weiblich / <=keine Angabe).

Die Adresse (*Bst. b*) und der Beruf (*Bst. c*), die nicht im Ausweis stehen, sind gemäss den Kundenangaben zu erfassen und auf ihre Plausibilität zu prüfen, also keine Fantasieangaben oder offensichtlich falsche Angaben. Es ist die Adresse – jeweils mit Strasse und Nummer - des Wohnsitzes, der Zweitwohnung, des Wochenaufenthalts oder des gewöhnlichen Aufenthalts zu erfassen, an welche die Kundin oder der Kunde kontaktiert wird.

Absatz 3 entspricht dem bisherigen Artikel 20 Absatz 4. Die FDA und die professionellen Wiederverkäuferinnen sind verpflichtet, bei Kundenbeziehungen ohne Abonnementsverhältnis (Prepaid, Gratisangebote) weitere Angaben zu erfassen. Nicht betroffen sind die einfachen vorbezahlten Telefonkarten, die zum Telefonieren verwendet werden können, aber keine SIM-Karten oder ähnliches sind. Der Grund für die Erfassung dieser weiteren Angaben liegt darin, dass nachvollziehbar sein muss, wer allfällige Falschregistrierungen vorgenommen hat (s. a. die entsprechende Strafbestimmung in Art. 39 Abs. 1 Bst. c BÜPF). Angemerkt sei, dass die FDA bei einer falsch registrierten Kundenbeziehung ohne Abonnementsverhältnis (Prepaid, Gratisangebote) den betreffenden Zugang zu Fernmeldediensten sperren muss (Art. 6*a* FMG). Mit dem Zeitpunkt nach *Buchstabe a* sind Datum und Uhrzeit gemeint. Name und Adresse nach *Buchstabe b* sind vollständig zu erfassen und richten sich danach, wer die Erfassung vornimmt, zum Beispiel ein Ladengeschäft einer Wiederverkäuferin, ein Callcenter der FDA, die die Aktivierung vornimmt oder eine Poststelle, die die Identitätsprüfung vornimmt. Bei Video- oder Online-Identifizierung sind Name und Adresse der für die Identifizierung verantwortlichen Stelle zu erfassen. Weiterhin sind gemäss *Buchstabe c* Namen und Vornamen der erfassenden Person respektive der für die Video- oder Online-Identifizierung verantwortlichen Person vollständig zu erfassen. Mit «erfassende Person» ist die Person gemeint, die die Angaben nach Absatz 3 tatsächlich erfasst oder, falls die Erfassung automatisch erfolgt, die für die Erfassung der Angaben verantwortlich ist (s. a. die entsprechende Strafbestimmung in Art. 39 Abs. 1 Bst. c BÜPF).

Der *erste Satz* von *Absatz 4* verlangt, dass das vorgelegte Ausweisdokument, bei dem es sich um das Original handeln muss, von der Anbieterin respektive von der professionellen Wiederverkäuferin kopiert werden muss, wie dies bereits heute gehandhabt wird. Diese Massnahme ist weiterhin notwendig, weil in der Vergangenheit viele Falschregistrierungen von Angaben zur Person stattgefunden haben. Die Ausweiskopie erscheint zurzeit als das geeignetste Mittel, um solchen Falschregistrierungen vorzubeugen. Es muss eine gut lesbare elektronische Ausweiskopie angefertigt werden

(z. B. Fotografie, Scan). Papierkopien genügen den neuen Anforderungen nicht mehr. Die Aufbewahrungsdauer für die FDA ist in Artikel 21 Absatz 4 geregelt. Im *zweiten Satz* wird eine Frist für die professionellen Wiederverkäuferinnen eingefügt, damit diese alle erfassten Angaben nach den Absätzen 2 und 3 sowie die Ausweiskopie zur FDA weiterleiten. Die Frist wird aus folgendem Grund auf 3 Tage festgelegt: Wenn Rufnummern erworben und kurz nach dem Verlassen des Geschäftes bereits genutzt werden, können sie am selben Tag ermittlungsrelevant werden. Deshalb ist es wichtig, dass die erfassten Angaben und die Ausweiskopie den Strafverfolgungsbehörden möglichst schnell in der IRC zur Verfügung stehen. Die Einhaltung der Frist von 3 Tagen erscheint auch für kleinere professionelle Wiederverkäuferinnen zumutbar. Mit diesem Absatz sollen die Verantwortlichkeiten klarer abgegrenzt werden (s. a. die entsprechende Strafbestimmung in Art. 39 Abs. 1 Bst. c BÜPF).

Art. 20b Erbringung des Identitätsnachweises bei juristischen Personen bei Mobilfunkdiensten

Absatz 1 regelt, welche Angaben bei den juristischen Personen zu erfassen sind. Sie entsprechen denjenigen im geltenden Artikel 20 Absatz 3. In der Regel werden die Angaben gemäss Auszug aus dem Handelsregister oder gemäss UID-Register des Bundesamts für Statistik erfasst. Neu kann auch der internationale Legal Entity Identifier (LEI) gemäss dem globalen Identifikationssystem für Finanzmarktteilnehmer erfasst werden (*Bst. b*). Bei juristischen Personen ist grundsätzlich die UID oder LEI zu erfassen. Die in *Buchstabe c* erwähnte Person, die die Dienste der Anbieterin in Anspruch nimmt, könnte zum Beispiel ein Mitarbeitender sein, der die SIM-Karte von ihrem Arbeitgeber erhält.

Absatz 2 entspricht Artikel 20*a* Absatz 4 zweiten Satz.

In *Absatz 3* wird auf Artikel 20*a* Absatz 3 («Kundenbeziehungen ohne Abonnementsverhältnis») verwiesen.

Art. 20c Abgabe von Zugangsmittel und Aktivieren von Diensten für Polizeibehörden und den NDB

Die Polizeibehörden und der NDB sind zur Erfüllung ihrer gesetzlichen Aufgaben bisweilen darauf angewiesen, fernmeldetechnische Zugangsmittel (z. B. Prepaid SIM-Karten) und Dienste einsetzen zu können, bei welchen diese Behörden und ihre Mitarbeitenden weder in den öffentlichen Verzeichnissen nach Artikel 12*d* FMG noch in den Daten der Verzeichnisse nach Artikel 21 FMG noch in der IRC aufscheinen dürfen. Sie brauchen solche Zugangsmittel namentlich zum Schutz ihrer Mitarbeitenden, ihrer Kontakte und Quellen, aber auch ihrer technischen Methoden und Fähigkeiten (z. B. bei der Kommunikation während Observationen von Personen mit Zugang zu fortgeschrittenen technischen Mitteln wie in Kreisen der organisierten Kriminalität oder der Spionage).

Der speziellen Schutzmassnahmen bedürfen diejenigen Mitarbeitenden der Polizeibehörden und des NDB, die ihre gesetzlichen Aufgaben unter Verwendung ihrer wahren Identität erfüllen, also ohne den Schutz durch eine Tarnidentität. Mitarbeitende mit einer solchen Tarnidentität (verdeckte Ermittlerinnen und Ermittler nach Art. 285*a* StPO und mit einer Tarnidentität ausgestattete Personen nach Art. 17 und 18 NDG)

können fernmeldetechnische Zugangsmittel unter Verwendung dieser Tarnidentität nach dem normalen Verfahren erwerben, ohne ihre wahre Identität offenlegen zu müssen und sind dadurch ausreichend geschützt. Der normale Bezug solcher Mittel kann dabei die Wirkung der Tarnung noch unterstützen.

Die Veröffentlichung der Kundendaten in öffentlichen Verzeichnissen ist nach Artikel 12*d* FMG ohnehin nicht verpflichtend. Die Kundinnen und Kunden haben diesbezüglich die Wahlfreiheit. Bei den FDA und den professionellen Wiederverkäuferinnen hat indessen eine grosse und nicht kontrollierbare Anzahl an Personen Zugriff auf deren Systeme und somit auf die Daten, welche zur Erteilung der Auskünfte gespeichert werden.

Gestützt auf die vorliegende Bestimmung haben die FDA zwar die Kenntnis, dass berechtigte Behörden Teilnehmende von bestimmten geschützten Zugangsmitteln und Diensten sind, sie sind aber gleichzeitig verpflichtet, diese Daten bestmöglich zu schützen und nur berechtigten Behörden auf Anfrage über den Dienst ÜPF bekannt zu geben. Die FDA erfüllen damit alle ihre Pflichten gemäss den Artikeln 21 ff. BÜPF betreffend die Identifikation der Teilnehmenden und der Auskunftserteilung an berechtigte Behörden, verhindern aber eine Kenntnisnahme durch potentielle Kriminelle und schützen so die operativen Tätigkeiten von Polizeibehörden und NDB.

Absatz 1 sieht aus obigen Gründen und Umständen nun neu vor, dass ein Vertrag zwischen einer FDA und einer Behörde abgeschlossen wird, wobei der Dienst ÜPF dabei die Rolle des Vermittlers einnimmt. Beim Vertrag handelt es sich nicht um den Abonnementsvertag selber, sondern um einen zusätzlichen Vertrag zwischen einer FDA und einer Behörde, der die Modalitäten für die Abgabe von Zugangsmittel und die Aktivierung von Diensten vorsieht. Um einen bestmöglichen und einheitlichen Schutzstandard zu gewährleisten, legen die FDA die Methoden im Einvernehmen mit dem Dienst ÜPF fest, um eine weitere Verbreitung der Daten zu verhindern. Es ist wichtig, den Kreis der Personen, die den Zugang zur Information über den wahren Inhaber haben, auf ein absolutes Minimum zu beschränken. Das Vorgehen wird dabei voraussichtlich vergleichbar sein wie bei der Sperrung der Daten von politisch exponierten Personen, die die FDA schon heute praktizieren.

Absatz 2 regelt den Ablauf der Abgabe von Zugangsmitteln und der Aktivierung von Diensten an Polizeibehörden und an den NDB nach dieser Bestimmung. Die Behörde (Polizeibehörde oder NDB) benennt aus ihren Reihen eine verantwortliche Person, die im Namen der Behörde berechtigt ist, bei der FDA Zugangsmittel zu beziehen oder Dienste aktivieren zu lassen. Diese Person kann für die berechtigte Behörde die Zugangsmittel beziehen und die Dienste aktivieren lassen und kennt die behördeninternen Benutzenden derselben. Seitens der FDA dokumentiert die zuständige Person intern die an die Behörden abgegebenen Zugangsmittel und aktivierten Dienste. So ist die FDA in der Lage, auf Anfrage des Dienstes ÜPF ihrer Verpflichtung zur Auskunftsgabe über die Teilnehmenden nachzukommen und könnte sich entlasten für den Fall, dass eine Anzeige gestützt auf Artikel 39 Absatz 1 Buchstabe c BÜPF beim Dienst ÜPF eingereicht werden sollte.

Absatz 3 hält fest, dass die berechtigten Behörden diese Zugangsmittel und Dienste nur im Rahmen der einschlägigen rechtlichen Bestimmungen (z. B. gemäss Art. 298*a* ff. StPO [verdeckte Fahndung] oder gemäss Art. 7 und 35 NDG) benützen

dürfen. Der Bezug von Zugangsmittel und Diensten nach den allgemeinen Voraussetzungen von Artikel 20*a* und 20*b* bleibt den Polizeibehörden und dem NDB weiterhin möglich.

Art. 21 Aufbewahrungsfristen

Dieser Artikel wurde umfassend überarbeitet, um die Regelungen der Aufbewahrungsfristen für die einzelnen Datenkategorien besser zu strukturieren, zu ergänzen und zu präzisieren. Hier wird geregelt, welche MWP die jeweiligen Daten für wie lange aufbewahren müssen. Die prinzipiellen Aufbewahrungsfristen werden nicht geändert, das heisst, Bestandsdaten (*subscriber data*) sind wie bisher während der Dauer der Kundenbeziehung zuzüglich 6 Monate nach deren Beendigung (Abs. 1 und 4) aufzubewahren. Identifikationsangaben der Benutzenden von professionell betriebenen öffentlichen WLAN-Zugängen sind während der Dauer der Zugangsberechtigung zuzüglich 6 Monate nach deren Ende (Abs. 2) und nutzungsabhängige Daten (*usage data*) sind während 6 Monaten ab Entstehung (Abs. 3) aufzubewahren. Die bisherige allgemeine Bezeichnung *Angaben zum Zweck der Identifikation* wird neu jeweils in den einzelnen Absätzen (Abs. 1, 3 und 5) präzisiert.

Absatz 1 entspricht dem bisherigen Absatz 1 erster Satz. Die Aufbewahrungspflicht für Daten (*Bst. a*) gilt für alle MWP, welche aktive Auskunftspflichten haben (alle FDA und die AAKD mit weitergehenden Pflichten gemäss Art. 22 oder 52). Neu hinzugefügt wurde die Aufbewahrungspflicht für Angaben über längerfristig zugeordnete Identifikatoren für Auskünfte gemäss Artikel 48*a* (*Bst. b*). Sie gilt nur für FDA, da die vorgenannten AAKD von Artikel 48*a* befreit sind (s. Art. 18 Abs. 4).

Absatz 2 gilt nur für die FDA, da es sich hierbei um einen Netzzugang handelt und entspricht der bisherigen Regelung mit einer redaktionellen Anpassung («WLAN-Zugang» statt «WLAN-Zugangspunkt»; s. Erläuterungen zum Ersatz von Ausdrücken, Abs. 1). Ausserdem wird die Präzisierung hinzugefügt, dass nur die professionell betriebenen WLAN-Zugänge betroffen sind (s. auch die einleitenden Erläuterungen zu diesem Artikel).

Absatz 3 betrifft ebenfalls nur die FDA, da es sich hierbei um einen Netzzugang handelt, und regelt die Aufbewahrung von Daten über die eindeutige Zuteilung von IP-Adressen (Art. 37). Bisher waren die Daten über die Zuteilung und Übersetzung von IP-Adressen und Portnummern (Art. 37, 38 und 39) im bisherigen Absatz 2 Buchstabe b gemeinsam enthalten. Aufgrund der Verhältnismässigkeit ist bei der dynamischen Zuteilung von IP-Adressen jedoch zwischen der eindeutigen Zuteilung von IP-Adressen (Art. 37) und der mehrdeutigen Zuteilung und Übersetzung (NAT) von IP-Adressen und Portnummern (Art. 38 und 39) zu unterscheiden (s. neuen Abs. 5 Bst. b). Bei den eindeutig zugeteilten IP-Adressen gibt es die fest zugeteilten (fixen) und die dynamisch zugeteilten IP-Adressen. Die Aufbewahrungsfrist für Daten über die Zuteilung von fixen IP-Adressen umfasst, wie bei allen Bestandsdaten, die gesamte Dauer der Kundenbeziehung zuzüglich 6 Monate (Abs. 1). Bei den dynamisch zugeteilten IP-Adressen beträgt die Aufbewahrungsfrist der Zuteilungsdaten jedoch nur 6 Monate (Abs. 3), da sie zu den nutzungsabhängigen Daten gehören. Der Unterschied besteht in der Zuteilung unabhängig von ihrer Nutzung bei fixen IP-Adressen

(die IP-Adresse ist während der Nutzungsdauer ständig zugeteilt, egal ob der entsprechende Internetzugang tatsächlich benutzt wird oder nicht). Bei dynamischer Zuteilung einer IP-Adresse erfolgt die Zuteilung nur dann, wenn der Internetzugang tatsächlich benutzt wird und ist damit nutzungsabhängig. Die gleiche IP-Adresse kann zu unterschiedlichen Zeitpunkten unterschiedlichen Teilnehmenden zugeteilt sein. Sie wird aber nie mehreren Teilnehmenden gleichzeitig zugeteilt (daher «eindeutig» zugeteilt).

In *Absatz 4* wird die Aufbewahrungsfrist für die Angaben über die Teilnehmenden und für die Kopie des Identitätsnachweises im Mobilfunkbereich explizit geregelt. Die Aufbewahrungspflicht für diese Daten gilt nur für FDA, welche Mobilfunkdienste anbieten (Mobilfunkanbieterinnen). Zu diesen Daten gehören die bei der Registrierung erfassten Angaben zur Person und bei natürlichen Personen auch die elektronische Kopie des Identitätsnachweises. Bisher wurde all dies lediglich implizit im bisherigen Absatz 1 subsumiert.

Bei den Daten nach *Absatz 5* handelt es sich um Daten zur Identifikation nach Artikel 22 Absatz 2 zweiter Satz BÜPF und von der Art her um Randdaten. Die Aufbewahrungspflicht für diese Daten ist mit der Randdatenaufbewahrung für die rückwirkende Überwachung vergleichbar. Aufgrund der grossen Datenmengen und des beträchtlichen Aufwands sind im Sinne der Verhältnismässigkeit nur die grossen FDA zur Aufbewahrung dieser Daten verpflichtet.

Dieser Absatz baut auf dem bisherigen Absatz 2 auf. *Buchstabe a* bleibt unverändert (nur die Verweise zu den entsprechenden Bestimmungen sind angepasst). *Buchstabe b* entspricht dem ehemaligen Buchstaben b, enthält aber die Daten zur Identifikation nach Artikel 37 (eindeutig zugeteilte IP-Adressen) nicht mehr, da diese gesondert in Absatz 3 geregelt werden. Neu regelt *Buchstabe c* die Aufbewahrungsfrist für die Randdaten zur Bestimmung der unmittelbar benachbarten Netze für Auskünfte gemäss Artikel 48*c* (s. die dortigen Erläuterungen). Durch den Entfall des Wortes *liefern* («während 6 Monaten aufbewahren» statt «während 6 Monaten aufzubewahren und zu liefern») wird klargestellt, dass diese Daten zur Identifikation aufzubewahren, aber im Rahmen von Auskünften nicht zu liefern sind, sofern sie nicht explizit Teil der zu liefernden Daten des Auskunftstyps sind. Die nicht zu liefernden Randdaten dienen in diesem Fall lediglich den MWP zur Auswertung und Durchführung der Identifikation der Benutzerschaft. Zu liefern sind nur die gemäss Auskunftsgesuch geforderten Angaben über den identifizierten Teilnehmenden (Art. 38) oder den identifizierten NAT-Übersetzungskontext (Art. 39). Die übrigen Randdaten dürfen von den MWP nur im Rahmen von Überwachungen (Echtzeit oder rückwirkend) geliefert werden, wobei die Randdaten nach Buchstabe b nicht Teil von standardisierten Überwachungstypen sind.

Die Daten nach *Absatz 6* entsprechen von der Art her den Daten in Absatz 5 Buchstaben a und b und es gilt die gleiche Aufbewahrungsfrist. Zur besseren Lesbarkeit wird dieser Absatz getrennt für die AAKD mit weitergehenden Überwachungspflichten (Art. 52) geregelt, da Absatz 5 Buchstabe c für sie nicht zutrifft. Sinngemäss gelten die entsprechenden Erläuterungen zu Absatz 5 Buchstaben a und b.

Absatz 7 entspricht dem bisherigen Absatz 3 mit der nötigen Anpassung des Verweises. Er regelt die Vernichtung der Randdaten, die in Absatz 5 näher umschrieben sind. Dies betrifft alle Anbieterinnen (Abs. 5 und 6), die diese Randdaten aufbewahren.

Es ist darauf hinzuweisen, dass über kurzzeitig zugeordnete Identifikatoren gemäss dem neuen Artikel 48*b* keine Angaben aufbewahrt werden müssen. Abfragen dieses Auskunftstyps sind aufgrund des sehr dynamischen Ablaufs dieser Zuordnungen nur echtzeitnah möglich (s. Erläuterungen zu Art. 48*b*).

Art. 26 Auskunftstypen

Absatz 1 dieses Übersichtsartikels wird formell umstrukturiert. Um die Lesbarkeit zu verbessern, wird auf die Nummerierung in Ziffern zugunsten einer neu etwas umfangreicheren Aufzählung in Buchstaben verzichtet.

In *Buchstabe d* wird der spezifische Begriff «Ausweiskopie» durch den allgemeineren Begriff «Identitätsnachweis» ersetzt, da neu auch elektronische Identitäten verwendet werden können. In *Buchstabe h* werden die zwei neuen Auskunftstypen gemäss Artikel 48*a* (IR_51_ASSOC_PERM: Auskünfte über längerfristig zugeordnete Identifikatoren) und Artikel 48*b* (IR_52_ASSOC_TEMP: sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren) und in *Buchstabe i* der neue Auskunftstyp gemäss Artikel 48*c* (IR_53_TEL_ADJ_NET, Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten) genannt.

In *Absatz 2* wird eine redaktionelle Änderung vorgenommen. Die Verwendung des Begriffs «Mitwirkungspflichtige» (MWP) statt des spezifischen Begriffs «Anbieterin» ist hier angezeigt. Auch die Betreiberinnen von internen Fernmeldenetzen (Art. 2 Bst. d BÜPF) und die Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen (Art. 2 Bst. e BÜPF), müssen Auskünfte erteilen. Diese sind aber keine Anbieterinnen, sondern werden unter dem allgemeineren Oberbegriff MWP subsumiert. Diese Regelung gilt auch, wenn die betreffende MWP aufgrund ihrer geringeren Pflichten keine standardisierten Auskünfte erteilen muss, sondern diese auch formlos erteilen kann.

Art. 28 Überwachungstypen

Dieser Übersichtsartikel wird mit den vier neuen Überwachungstypen zur Positionsbestimmung (zwei zur Echtzeitüberwachung, zwei zur Notsuche) ergänzt und es werden Anpassungen an den Titeln von bereits existierenden Überwachungstypen vorgenommen. Ausserdem wird er formell umstrukturiert, um die Lesbarkeit zu verbessern. Die bisherige Absatzstruktur entfällt und die bisherigen Absätze 1–5 werden neu zu den *Buchstaben a–e*. Dadurch werden die bisherigen Buchstaben in den Substrukturen neu zu Ziffern.

Buchstabe a Ziffern 1-3 bleiben im Wesentlichen unverändert. *Ziffer 4* wird neu eingefügt und verweist auf die beiden neuen Typen der Echtzeitüberwachung zur Positionsbestimmung (LALS, s. Art. 56*a* und 56*b*). Dadurch wird der bisherige Buchstabe d zu *Ziffer 5*.

In *Buchstabe b Ziffer 3* heisst es neu «die Bestimmung des Standorts bei der letzten Aktivität» (s. auch die Erläuterungen zu Art. 63).

In *Buchstabe c Ziffer 1* hat sich der Titel der Notsuche wie folgt geändert: die Bestimmung des Standorts bei der letzten Aktivität (s. Art. 67 Bst. a). *Ziffer 2* wird neu eingefügt und verweist auf die beiden neuen Typen der Notsuche zur Positionsbestimmung (LALS, s. Art. 67 Bst. b und c). *Ziffern 3*, *4* und *5* bleiben unverändert und entsprechen den bisherigen Buchstaben b, c und d des bisherigen Absatzes 3. Nur die Verweise zu den entsprechenden Bestimmungen in Klammern sind angepasst.

In *Buchstabe d Ziffer 1* heisst es neu «die Bestimmung des Standorts bei der letzten Aktivität» (s. auch die Erläuterungen zu Art. 63). *Ziffer 2* wird neu eingefügt und verweist auf die beiden neuen Typen der Fahndung zur Positionsbestimmung durch das Netzwerk (LALS, s. Art. 68 Abs. 1 Bst. b und c). *Ziffern 3, 4 und 5* bleiben unverändert und entsprechen den bisherigen Buchstaben b, c und d des bisherigen Absatzes 4. Nur die Verweise zu den entsprechenden Bestimmungen in Klammern sind angepasst. In *Ziffer 6* wird der Verweis auf den bereits existierenden Antennensuchlauf im Rahmen einer Fahndung (Art. 68 Abs. 1 Bst. g, bisher Bst. d) nachgetragen.

Buchstabe e wurde leicht gekürzt und entspricht inhaltlich dem bisherigen Absatz 5, der mit der VPMT[22] am 1. Juni 2022 in Kraft getreten ist.

Art. 30 Abs. 3

Absatz 3 wird mit einem zweiten Satz ergänzt, wonach die MWP dem Dienst ÜPF die Durchführung von notwendigen Testschaltungen ermöglichen. Diese Ergänzung ist notwendig, da es Fälle gibt, in denen die MWP die Testschaltungen nicht zur Verfügung stellen können, wie es im ersten Satz geregelt ist. In diesen Fällen führen der Dienst ÜPF oder von diesem beauftragte Personen die Testschaltungen durch. Dies ist insbesondere bei MWP der Fall, die keine aktiven Überwachungspflichten haben (d.h. keine Überwachungsbereitschaft herstellen müssen). Testschaltungen können auch bei besonderen Überwachungen (Art. 25), sogenannten Spezialfälle durchgeführt werden. Neben der Duldung der angeordneten Überwachung, die durch den Dienst ÜPF oder durch von diesem beauftragte Personen durchgeführt wird (Art. 26 Abs. 2 Bst. b BÜPF), gehört es zu den notwendigen Nebenpflichten der MWP (s. Botschaft vom 27.02.2013 zum BÜPF zu Art. 26 Abs. 2, BBl 2013 2740), im Zusammenhang mit einer angeordneten Überwachung dem Dienst ÜPF die Durchführung von Testschaltungen zu ermöglichen, beispielsweise um die korrekte Funktion der angeordneten Überwachung zu überprüfen. Für die Durchführung von Testschaltungen müssen die MWP dem Dienst ÜPF oder den von diesem beauftragten Personen unverzüglich den Zugang zu ihren Anlagen gewähren (s. Art. 53 Abs. 1).

Art. 35 Abs. 1 Bst. b, c und d Einleitungssatz und Ziff. 2, 9–13, Abs. 2 Einleitungssatz und Bst. g und i–k sowie Abs. 3

In *Absatz 1 Buchstabe b* werden die zu liefernden Angaben übersichtlicher in 3 Ziffern gegliedert. In *Ziffer 1* werden die Verweise angepasst. Neu sind in Artikel 20 die Überprüfung der Teilnehmerangaben bei Mobilfunkdiensten, in Artikel 20*a* die entsprechende Erbringung des Identitätsnachweises bei natürlichen Personen und in

22 Verordnung vom 04.05.2022 über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (**VPMT**; AS **2022** 301)

Artikel 20*b* die entsprechende Erbringung des Identitätsnachweises bei juristischen Personen geregelt. In *Ziffer 2* werden «weitere Adressen» und der Gültigkeitszeitraum der «weiteren Adressen und Kontaktdaten» hinzugefügt. Bei den Anbieterinnen werden oft nicht nur die Adresse zum Zeitpunkt der Registrierung, sondern auch Folgeadressen nach einem Umzug und andere Adressen der Teilnehmenden, wie eine abweichende Zustelladresse oder Rechnungsadresse, gespeichert. Als «weitere Kontaktdaten» kann die MWP beispielsweise weitere ihr bekannte Telefonnummern und E-Mail-Adressen des Teilnehmenden mitteilen. Mit Gültigkeitszeitraum ist die Zeitspanne (Datum des Beginns und gegebenenfalls des Endes) gemeint, von wann bis wann die jeweiligen Adressen und weiteren Kontaktdaten bei der MWP gemeldet sind beziehungsweise waren. Die MWP gibt die bei ihr vorhandenen Daten und Gültigkeitszeiträume bekannt. Sie hat keine Pflicht zur lückenlosen Erfassung und Nachführung der weiteren Adressen und Kontaktdaten ihrer Teilnehmenden.

In *Buchstabe c* werden sinngemäss die gleichen Änderungen vorgenommen, wie in Buchstabe b. Es entfällt jedoch die Anpassung der Verweise in Ziffer 1, da sich diese nur für Mobilfunkdienste ändern. Buchstabe c ist auf alle Netzzugangsdienste anwendbar, die keine Mobilfunkdienste sind. Ergänzend ist anzumerken, dass wie bisher die bei der Identifizierung mit geeigneten Mitteln gemäss Artikel 19 erfassten Angaben zu liefern sind. In der Praxis hat sich gezeigt, dass aufgrund der Vielzahl der Möglichkeiten dieser Identifizierung und Datenerfassung hier keine feste Datenstruktur vorgegeben werden kann. Die Angaben können daher unstrukturiert übermittelt werden, sind jedoch mit einer geeigneten Bezeichnung zu versehen, damit die berechtigten Behörden besser verstehen können, was die übermittelten Angaben bedeuten (z. B. MSISDN, Kreditkartennummer, Ausweisnummer, ID-Nummer, Boardingpass, MRZ, IPASS Username).

Im Einleitungssatz des *Buchstabens d* wird eine redaktionelle Änderung im Sinne der geschlechtergerechten Sprache vorgenommen.

In *Ziffer 2* erfolgen zwei Änderungen. Erstens wird der bisherige Begriff *Dienstidentifikator* durch *Haupt-Dienstidentifikator* ersetzt, da es Mobilfunkabonnemente mit mehreren Nummern oder mehreren SIM-Karten gibt, die gleichzeitig in verschiedenen Endgeräten betrieben werden können (sog. Multi-SIM- oder Multi-Device-Angebote). Dadurch entsteht eine Hierarchie innerhalb des Abonnements: eine Hauptnummer (Master) und weitere Nebennummern (Slaves). Diese Hierarchie kann von dem oder der Teilnehmenden selbst geändert werden, das heisst er oder sie kann selbst bestimmen, welche SIM-Karte oder welches Gerät gerade die Hauptnummer oder die Nebennummern benutzt. Dadurch können einer IMSI beispielsweise mehrere MSISDN zugeordnet sein. Im einfachen Fall ist einer IMSI nur eine MSISDN zugeordnet. Die Nebennummern können auch technische Nummern sein, die dem oder der Teilnehmenden in der Regel nicht bekannt sind. Diese Multi-SIM- oder Multi-Device-Angebote haben Auswirkungen auf die Auskunftserteilung, die Überwachungen, Notsuchen und Fahndungen.

Zweitens ersetzt ein neuer Identifikator des 5G-Systems, der *Generic Public Subscription Identifier* (GPSI), den bisher beispielhaft genannten *DSL-Identifikator* von Breitbandinternetanschlüssen im Festnetz, da der *GPSI* verhältnismässig an Bedeutung gewinnt. In den Beispielen dieser Verordnung wird daher überall der *DSL-Identifikator* durch den *GPSI* ersetzt, da die Beispiele möglichst typisch und aktuell sein sollen.

Das heisst aber nicht, dass der *DSL-Identifikator* nicht mehr geliefert werden muss (gilt auch für alle anderen ersetzten Beispiele). *GPSI* sind öffentliche Identifikatoren, die sowohl innerhalb, als auch ausserhalb des 3GPP-Systems verwendet werden. Der *GPSI* ist entweder eine MSISDN (z. B. +41791234567) oder ein externer Identifikator der Form <username>@<domain_name> (z. B. max.maier@mnc999.mcc228.csp.ch). Der GPSI wird insbesondere für die Adressierung eines 3GPP-Dienstes in Netzen ausserhalb des 3GPP-Systems benötigt, zum Beispiel wenn die Benutzenden nicht das Mobilfunknetz, sondern einen Nicht-3GPP-Zugang (WLAN) als Netzzugang benützen. Der Zusatz 3GPP bedeutet jeweils, dass es sich um ein von der 3GPP standardisiertes Mobilfunksystem (*3GPP-System*) beziehungsweise Dienst (*3GPP-Dienst*) handelt.

Ein weiterer Identifikator, der nicht in den Beispielen erwähnt wird, der jedoch falls zutreffend geliefert werden muss, ist der OTO-ID, der einen Glasfaser-Heimanschluss (Fiber to the home) eindeutig bezeichnet.

Ziffer 9 bleibt inhaltlich unverändert. Es wird lediglich der Begriff SIM-Nummer durch den universellen Fachbegriff ICCID (im Anhang definiert) ersetzt, da die Funktion der klassischen SIM-Karte auch durch andere Hardware (z. B. embedded SIM, eSIM) übernommen werden kann und nicht immer zweifelsfrei feststeht, was genau mit SIM-Nummer gemeint ist. Der Begriff ICCID ist dagegen eindeutig für alle Formen von SIM.

In *Ziffer 10* wird neben der bisherigen *IMSI* neu der vergleichbare Identifikator des 5G-Systems *SUPI* eingefügt. Im 5G-System wird jedem Teilnehmenden ein Subscription Permanent Identifier (SUPI) zugewiesen. Der *SUPI* ist weltweit eindeutig und wird in der Teilnehmerdatenbank des Heimnetzes (UDM/UDR) eingerichtet. Der *SUPI* wird nur innerhalb des 3GPP-Systems benutzt. Als *SUPI* kann beispielsweise die *IMSI* verwendet werden. Das Endgerät kann dem Netz seinen *SUPI* in verschlüsselter Form mitteilen (z. B. bei der Anmeldung im Netz), was Auswirkungen auf den Einsatz besonderer technischer Geräte zur Überwachung gemäss Artikel 269bis StPO hat (s. Art. 48*b*). Um Roaming zu ermöglichen, enthält der *SUPI* die Adresse des Heimnetzes (z. B. Mobile Country Code *MCC* und Mobile Network Code *MNC*). Das 5G-System speichert in der Teilnehmerdatenbank die Beziehung zwischen *GPSI* und zugehörigen *SUPI*, wobei diese Beziehung nicht notwendigerweise 1:1 sein muss (die Abfrage der aktuell zugehörigen *GPSI* bzw. *SUPI* kann mit einem Auskunftsgesuch gemäss Art. 36 oder 41 erfolgen).

Ziffer 11 wird korrigiert. Aufgrund eines Versehens bei der Übersetzung aus dem englischen ETSI-Standard stand irrtümlicherweise bisher «Typ des Dienstes». Es muss jedoch «Typ der Kundenbeziehung» (engl. «subscription type») heissen. Inhaltlich ändert sich nichts.

Ziffer 12 wird präzisiert. Wie oben bei Ziffer 2 erläutert, kann es noch weitere Adressierungselemente (z. B. Telefonnummer «MSISDN») und Dienstidentifikatoren (z. B. SIM-Nummer «ICCID») geben, die zum angefragten Netzzugangsdienst (z. B. Mobilfunkabonnement) gehören. Diese sind in diesem Feld in Form einer Liste oder als Bereichsangabe (Range, von-bis) mitzuteilen. Dazu gehören auch erst nach der Registrierung hinzugekommene Adressierungselemente und Identifikatoren, soweit sie

Teil der Bestandesdaten (*subscriber data*) sind. In Abhängigkeit der Benutzung (usage data) zugeordnete Adressierungselemente und Identifikatoren werden nicht hier, sondern mittels des Auskunftsgesuches nach Artikel 36 abgefragt. Neu ist der Gültigkeitszeitraum des jeweiligen Adressierungselements respektive Identifikators anzugeben.

In *Ziffer 13* wird ein Feld zur Übermittlung der Bezeichnung des angefragten Netzzugangsdienstes (z. B. Name des Produkts, Angebots, Abonnements oder Tarifs) eingefügt. Damit wird den auskunftsersuchenden Behörden die Auswertung der gelieferten Antworten erleichtert. Weiter hilft es ihnen besser zu verstehen, um was für einen Dienst es sich handelt. Hier kann beispielsweise die Verkaufsbezeichnung des Abonnements bekanntgegeben werden. Aufgrund der Vielzahl unterschiedlicher Dienstangebote auf dem Markt wurde diese Ergänzung von Seiten der Strafverfolgungsbehörden gewünscht.

Die beiden Einleitungssätze des *Absatzes 2* wurden unverändert vom bisherigen Absatz 2 übernommen. In *Buchstabe g* wird bei der UID präzisiert, dass es sich um einen nationalen Identifikator handelt und neu kann die Anfrage auch mit dem LEI gestellt werden (s. Erläuterungen zu Art. 20*b* Abs. 1 Bst. b). In *Buchstabe i* wird der Teilnehmeridentifikator (z. B. Kundennummer) als Anfragekriterium hinzugefügt. Dies ist nützlich für die Abfrage aller Dienste eines bestimmten Teilnehmers oder für die Abfrage eines alternativen Teilnehmeridentifikators gemäss Artikel 36 Absatz 1 Buchstabe b Ziffer 3 (z. B. bei professionell betriebenem öffentlichem WLAN-Zugang). Ausserdem wird statt «DSL-Identifikator» ein anderes Beispiel (GPSI) für einen Dienstidentifikator erwähnt (s. Erläuterungen zu Abs. 1 Bst. d Ziff. 2). In *Buchstabe j* wird ein neuer Identifikator des 5G-Systems (SUPI) hinzugefügt (s. Erläuterungen zu Abs. 1 Bst. d Ziff. 10). In *Buchstabe k* entfällt der Begriff *SIM-Nummer* und wird durch den universellen Fachbegriff *ICCID* ersetzt (s. Erläuterungen zu Abs. 1 Bst. d Ziff. 9).

Der *erste Satz* von *Absatz 3* entspricht grundsätzlich dem dritten Satz des bisherigen Absatzes 2. Es wird lediglich eine Korrektur vorgenommen. Namentlich, das Anfragekriterium nach Buchstabe e (Ausweisnummer) wird nicht mehr in dieser Bestimmung aufgenommen. Da es sich bei diesem Anfragekriterium um ein eindeutiges Anfragekriterium handelt, muss bei dessen Verwendung in der Anfrage kein zweites Anfragekriterium angegeben werden. Der *zweite Satz* entspricht dem vierten Satz des bisherigen Absatzes 2.

Art. 36 Auskunftstyp IR_6_NA: Auskünfte über Netzzugangsdienste

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen.

Absatz 1 wird neu strukturiert mit *Buchstabe a* (unverändert) und *Buchstabe b*, der in den Ziffern 1 bis 6 die zu liefernden Angaben pro Dienst vorgibt. Neben dem angefragten Dienst kann es noch weitere Dienste geben, die mit diesem zusammenhängen. Der bisherige zweite Einleitungssatz von Absatz 1 entfällt, da die Lieferung des Gültigkeitszeitraums bestimmter Angaben neu jeweils einzeln geregelt wird.

Ziffer 1 entspricht inhaltlich unverändert dem bisherigen Buchstaben b. *Ziffer 2* definiert die weiteren Dienstidentifikatoren, bei denen es sich nicht nur um die MSISDN,

sondern auch um andere Identifikatoren handeln kann. Dieser Auskunftstyp dient für alle Arten von Netzzugangsdiensten, nicht nur für Mobilfunk. Neu ist für die Dienstidentifikatoren nach Ziffer 2 der jeweilige Gültigkeitszeitraum zu liefern, damit die Strafverfolgungsbehörden deren zeitliche Relevanz erkennen können. *Ziffer 3* ist neu und dient zur Teilnehmeridentifikation bei professionell betriebenen öffentlichen WLAN-Zugängen. Mit dem hiermit erhaltenen Identifikator kann die berechtigte Behörde im nächsten Schritt ein Auskunftsgesuch IR_4_NA (Art. 35) stellen und bekommt dann die Identifikationsangaben gemäss Artikel 19 Absatz 2. *Ziffer 4* entspricht im Wesentlichen dem bisherigen Buchstaben d und regelt die zu übermittelnden Angaben über die im Zusammenhang mit dem jeweiligen Dienst bei der Anbieterin in den letzten 6 Monaten benutzten Geräte. Neu ist der «*Permanent Equipment Identifier*» (PEI), der zur 5G-Technologie gehört. Der PEI dient zur weltweit eindeutigen Identifikation von Endgeräten in 5G-Mobilfunknetzen. Der PEI besteht entweder aus einer IMEI oder einer IMEISV. *Ziffer* 5 fasst die bisherigen Buchstaben e (ICCID statt SIM-Nummer, s. Erläuterungen zu Abs. 1 Bst. d Ziff. 9) und f (PUK) zusammen und ergänzt sie mit dem Gültigkeitszeitraum und weiteren Identifikatoren wie IMSI und MSISDN, um den berechtigten Behörden einen besseren chronologischen Überblick über die zum jeweiligen Netzzugangsdienst gehörigen SIM-Karten und ähnliche Zugangsmittel zu geben. Neu sind die beiden Identifikatoren in 5G-Mobilfunknetzen: SUPI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10) und GPSI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2). Neu hinzugekommen ist *Ziffer 6*, die zur Übermittlung von Multi-Device-Informationen dient. Da die Zuordnung von Haupt- («Primary») und Nebengeräten («Secondary») jederzeit von den Benutzenden geändert werden kann, sind die Multi-Device-Informationen dynamisch und daher mittels IR_6_NA abzufragen, der sich auf die Nutzungsdaten stützt.

In *Absatz 2* sind wie bisher auch weiterhin nur diejenigen Angaben zu liefern, die im Anfragezeitraum gültig waren respektive sind. Da sich dieser Auskunftstyp auf Nutzungsdaten stützt, müssen die auskunftspflichtigen MWP die hier aufgeführten Daten nur während 6 Monaten aufbewahren. Bei länger als 6 Monate in die Vergangenheit reichenden Anfragen, müssen die MWP nur die bei ihnen allfällig noch vorhandenen Daten liefern.

In *Buchstabe a* wird in den Beispielen der DSL-Identifikator durch GPSI ersetzt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2) und es kommt neu die Möglichkeit hinzu, Abfragen mit einem Identifikator zu machen, der zur Teilnehmeridentifikation bei professionell betriebenen öffentlichen WLAN-Zugängen dient. Die *Buchstaben b* und *c* bleiben im Prinzip gleich, es werden lediglich neue Identifikatoren des 5G-Systems hinzugefügt: SUPI und PEI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10 bzw. Art. 36 Abs. 1 Bst. b Ziff. 4). *Buchstabe d* bleibt unverändert. *Buchstabe e* wird neu hinzugefügt, um insbesondere die Abfrage des PUK-Codes zu standardisieren und damit effizienter zu gestalten. Bisher waren dafür zwei Auskunftsgesuche IR_4_NA und IR_6_NA notwendig. Jetzt ist nur noch eine Abfrage IR_6_NA nötig, um den PUK-Code zu einer bestimmten ICCID abzufragen.

Art. 37 Abs. 1 Einleitungssatz und Bst. b

Im *Einleitungssatz* des *Absatzes 1* wird eine redaktionelle Änderung im Sinne der geschlechtergerechten Sprache vorgenommen.

In *Buchstabe b* wird in den Beispielen der DSL-Identifikator durch einen Identifikator des 5G-Systems (GPSI) ersetzt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2). Die neu eingefügte Alternative «einen Identifikator, der eine Anfrage der die Identifikationsangaben gemäss Artikel 19 Absatz 2 ermöglicht» dient zur Teilnehmeridentifikation bei professionell betriebenen öffentlichen WLAN-Zugängen. Mit dem hiermit erhaltenen Identifikator kann die berechtigte Behörde im nächsten Schritt ein Auskunftsgesuch IR_4_NA (Art. 35) stellen und bekommt dann die Identifikationsangaben gemäss Artikel 19 Absatz 2.

Art. 38 Abs. 1 Einleitungssatz und Bst. b sowie Abs. 2 Einleitungssatz und Bst. f

Der Einleitungssatz von *Absatz 1* ist verkürzt, ändert sich aber inhaltlich nicht. Die Formulierung «zum Zweck der Identifikation» entspricht der französischen Fassung. In *Buchstabe b* wird in den Beispielen der DSL-Identifikator durch einen Identifikator des 5G-Systems (GPSI) ersetzt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2). Die neu eingefügte Alternative «einen Identifikator, der eine Anfrage der Identifikationsangaben gemäss Artikel 19 Absatz 2 ermöglicht» dient zur Teilnehmeridentifikation bei professionell betriebenen öffentlichen WLAN-Zugängen (s. Erläuterungen zu Art. 37 Abs. 1 Bst. b).

In *Absatz 2* wird der Einleitungssatz so präzisiert, dass sich die Abfrage auf den gesamten «Übersetzungskontext» bezieht, statt auf einen einzelnen «Übersetzungsvorgang», da für den gesamten Übersetzungskontext die einzelnen NAT-Übersetzungen gleich sind. Der Zusatz «zum Zweck der Identifikation» kann hier entfallen, da er bereits in Absatz 1 steht.

Mit den Änderungen in *Buchstabe f* wird der Zeitpunkt (neu: massgeblicher Zeitpunkt) neu definiert. Gemäss dem Urteil des Bundesverwaltungsgerichts A-6807/2019 (Ziff. 4.5.1 S. 24) hat eine FDA die Randdaten über die Zuteilung und Übersetzung von IP-Adressen und Portnummern (vgl. Art. 21 Abs. 5 Bst. b VÜPF) in einer Weise zu speichern, die es ihr ermöglicht, die Benutzerschaft zu jedem von der auskunftsersuchenden Behörde verlangten Zeitpunkt zu identifizieren und die Angaben gemäss Artikel 38 Absatz 1 VÜPF zu liefern, sofern ihr die ersuchende Behörde die Angaben gemäss Artikel 38 Absatz 2 VÜPF für den gesuchten Zeitpunkt bekannt gibt. Mit dieser Änderung wird klargestellt, dass von der ersuchenden Behörde ein beliebiger Zeitpunkt zu Beginn, während oder am Ende eines bestimmten NAT-Übersetzungskontextes angefragt werden kann. Der massgebliche Zeitpunkt in der Anfrage muss also insbesondere nicht notwendigerweise nahe am Beginn des angefragten (beobachteten) NAT-Übersetzungskontextes liegen.

Dieser standardisierte Auskunftstyp erlaubt nur eindeutige Antworten, das heisst nur ein Identifikator ist zu finden. Falls die MWP mehrere passende Ergebnisse findet, dürfen diese nicht als Ergebnis dieses Auskunftstyps übermittelt werden. Diese Einschränkung ist wichtig, da dieser Auskunftstyp keine Möglichkeiten vorsieht, die Pertinenz der einzelnen Ergebnisse zu bewerten.

Art. 39 Auskunftstyp IR_9_NAT: Auskünfte über NAT-Übersetzungskontexte

In dieser Bestimmung werden zahlreiche kleinere Änderungen vorgenommen, auch um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. Im Unterschied

zu Artikel 38, in dem es um die üblichen Auskünfte zur Teilnehmeridentifikation im Zusammenhang mit NAT geht, stehen hier die ganz speziellen Aspekte des NAT im Vordergrund. Dieser Auskunftstyp dient Spezialisten für das sogenannte Backtracking von Verbindungen über NAT-Grenzen hinweg. Ausführliche Erläuterungen zu diesem Verfahren finden sich auf Seiten 43 und 44 des Erläuternden Berichts zur Totalrevision der VÜPF vom 15. November 2017.

Im Einleitungssatz von *Absatz 1* wird analog zu Artikel 38 neu präzisiert, dass sich die Abfrage auf den gesamten «Übersetzungskontext» bezieht, statt auf einen einzelnen «Übersetzungsvorgang», da für den gesamten Übersetzungskontext die einzelnen NAT-Übersetzungen gleich sind. Der materielle Inhalt der *Buchstaben a* und *b* ändert sich nicht, ausser dass der Ausdruck «NAT-Übersetzungsvorgang» zu «NAT-Übersetzung» vereinfacht wird. Inhaltlich macht das keinen Unterschied, da für den gesamten Übersetzungskontext die einzelnen NAT-Übersetzungen gleich sind.

In *Absatz 2* wird wie in Absatz 1 der Ausdruck «Übersetzungsvorgang» durch «Übersetzungskontext» ersetzt, da auch hier für den gesamten Übersetzungskontext die einzelnen NAT-Übersetzungen gleich sind. Weiter wird präzisiert, dass nicht alle, sondern nur die bekannten Angaben über den angefragten Übersetzungskontext in der Anfrage anzugeben sind. Die anfragende Behörde muss jedoch damit rechnen, dass die Anbieterin bei rudimentären Angaben nicht den richtigen Übersetzungskontext finden kann.

Der materielle Inhalt der *Buchstaben a-d* ändert sich nicht. In *Buchstaben* e wird die Präzisierung«falls für die Identifikation notwendig» hinzugefügt, da die Speicherung der Art des Protokolls aus Datenschutzgründen auf das notwendige Minimum begrenzt werden soll. In *Buchstabe f* wird der massgebliche Zeitpunkt analog zu Artikel 38 Absatz 2 Buchstabe f präzisiert (s. die dortigen Erläuterungen).

Art. 40 Abs. 1 Bst. b, c und d Einleitungssatz sowie Ziff. 2, 6, 7 und 10–13, Abs. 2 Einleitungssatz und Bst. g, j und k sowie Abs. 3

In *Absatz 1 Buchstaben b* und *c* wird der jeweilige Gültigkeitszeitraum für die weiteren Adressen und Kontaktdaten eingefügt (s. Erläuterungen zur analogen Änderung in Art. 35 Abs. 1 Bst. b und c).

In *Buchstabe d Ziffer 2* wird präzisiert, dass der Haupt-Dienstidentifikator zu liefern ist, beispielsweise die Hauptrufnummer. Diese Präzisierung ist erforderlich, da es Mobilfunkdienste mit Extra-SIM-Karten (z. B. Multi-Device, Multi-SIM) gibt, die mehr als einen Identifikator (z. B. MSISDN) haben. Die übrigen Identifikatoren sind unter Ziffer 7 zu liefern.

Gemäss *Buchstabe d Ziffer 6* können, ebenso wie beim Auskunftstyp IR_4_NA (nicht geänderter Art. 35 Abs. 1 Bst. d Ziff. 6), nun für die Zustände des Dienstes die jeweiligen Gültigkeitszeiträume mitgeteilt werden. Da der ETSI-Standard unterschiedliche Datenformate für Netzzugangsdienste (NA) und Multimediadienste (TEL) definiert, musste zunächst ein Änderungsantrag (Change Request) an das ETSI gestellt werden, um den bereits für Netzzugangsdienste (NA) vorhandenen Parameter Gültigkeitszeitraum auch für Multimediadienste (TEL) zu definieren. Nachdem das ETSI den Standard nun angepasst hat, kann diese Änderung hier vorgenommen werden.

In *Ziffer 7* wird der Zusatz «zugehörigen» eingefügt, um zum Ausdruck zu bringen, dass es sich auch um die zum angefragten Dienst zugehörigen (associated) Adressierungselemente (z. B. Telefonnummer) und Identifikatoren (z. B. SIM-Nummer «ICCID») handelt, beispielsweise bei Mobilfunkdiensten mit Extra-SIM-Karten. Dazu gehören auch erst nach der Registrierung hinzugekommene Adressierungselemente und Identifikatoren, soweit sie Teil der Bestandesdaten (*subscriber data*) sind. In Abhängigkeit der Benutzung (usage data) zugeordnete Adressierungselemente und Identifikatoren werden nicht hier, sondern mittels des Auskunftsgesuches nach Artikel 41 abgefragt. Neu ist der Gültigkeitszeitraum des jeweiligen Adressierungselements respektive Identifikators anzugeben.

In *Ziffer 10* wird der neue Identifikator des 5G-Systems SUPI eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10). Zudem wird neu von «zugehörigen» IMSI oder SUPI gesprochen, um zum Ausdruck zu bringen, dass es sich um mehrere IMSI oder SUPI handeln kann (Bsp. Mobilfunkdienste mit Extra-SIM-Karten).

In *Ziffer 11* entfällt der Begriff *SIM-Nummer* und wird durch den universellen Fachbegriff *ICCID* ersetzt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 9). Ausserdem wird der Zusatz «zugehörigen» eingefügt, um zum Ausdruck zu bringen, dass es sich um mehrere ICCID handeln kann (Bsp. Mobilfunkdienste mit Extra-SIM-Karten).

In *Ziffer 12* konnte bisher nicht in Analogie zu Artikel 35 Absatz 1 Ziffer 11 der «Typ der Kundenbeziehung» (engl. «subscription type») übermittelt werden, da der entsprechende ETSI-Standard zum Zeitpunkt der Erarbeitung der VÜPF vom 15. November 2017 noch nicht den notwendigen Parameter enthielt. Inzwischen wurde der Standard angepasst und die Übermittlung des «Typs der Kundenbeziehung» ist nun möglich.

In *Ziffer 13* wird ein Feld für die Übermittlung der «Bezeichnung des Dienstes» eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 13).

In *Absatz 2 Buchstabe g* wird hinzugefügt, dass neu die Anfrage auch mit dem LEI (s. Erläuterungen zu Art. 20*b* Abs. 1 Bst. b) gestellt werden kann.

In *Buchstabe j* wird ein neuer Identifikator des 5G-Systems (SUPI) eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10).

In *Buchstabe k* entfällt der Begriff *SIM-Nummer* und wird durch den universellen Fachbegriff *ICCID* ersetzt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 9).

Absatz 3 entspricht inhaltlich dem dritten und vierten Satz des bisherigen Absatzes 2, die aus redaktionellen Gründen in diesen neuen Absatz verschoben werden.

Art. 41 Auskunftstyp IR_12_TEL: Auskünfte über Telefonie- und Multimediadienste

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. Der bisherige zweite Einleitungssatz von *Absatz 1* entfällt, da die Lieferung des Gültigkeitszeitraums bestimmter Angaben neu jeweils einzeln geregelt wird.

Absatz 1 wird neu in zwei Buchstaben strukturiert. *Buchstabe a* bleibt unverändert. *Buchstabe b* wird neu in vier *Ziffern untergliedert,* in denen die zu liefernden Angaben pro Dienst vorgegeben werden. Neben dem angefragten Dienst kann es noch weitere

Dienste geben, die mit diesem zusammenhängen. Im Einleitungssatz wird der Zusatz «zugehörigen» eingefügt, um zum Ausdruck zu bringen, dass es sich auch um die zum angefragten Dienst zugehörigen («associated») Dienste mit ihren Adressierungselementen und Identifikatoren handelt, beispielsweise bei Mobilfunkdiensten mit Extra-SIM-Karten (z. B. Multi-Device, Multi-SIM), da diese mehr als einen Identifikator (z. B. MSISDN) haben. *Ziffer 1* entspricht im Prinzip dem bisherigen Buchstaben b. Neu ist die Unterscheidung zwischen öffentlichen und privaten Adressierungselementen und die Angabe des Gültigkeitszeitraums (Datum von – bis) des jeweiligen Adressierungselementes. *Ziffer 2* entspricht im Prinzip dem bisherigen Buchstaben d und regelt die zu übermittelnden Angaben über die im Zusammenhang mit dem jeweiligen Dienst bei der Anbieterin in den letzten 6 Monaten benutzten Geräte. Als Beispiel werden die IMEI und PEI aufgeführt, wie in Artikel 36 Absatz 1 Buchstabe b Ziffer 4. Die seltener vorkommende MAC-Adresse wir nicht mehr als Beispiel aufgeführt, gehört aber immer noch zu den Geräteidentifikatoren. *Ziffer 3* fasst die bisherigen Buchstaben c (IMSI), e (ICCID) und f (PUK) zusammen und ergänzt sie mit weiteren Identifikatoren wie SUPI, MSISDN und GPSI sowie eUICC ID und dem Gültigkeitszeitraum, um den berechtigten Behörden einen besseren chronologischen Überblick über die zum jeweiligen Dienst gehörigen Zugangsmittel (SIM) und Identifikatoren zu geben. Neu sind die beiden Identifikatoren in 5G-Mobilfunknetzen: SUPI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10) und GPSI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2). Neu wird der Begriff ICCID statt SIM-Nummer verwendet (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 9). *Ziffer 4* ist neu und dient zur Übermittlung der Angabe, ob es sich bei Multi-Device jeweils um das Hauptgerät oder ein Nebengerät handelt.

In *Absatz 2 Buchstabe a* werden die Beispiele gekürzt, das heisst Telefonnummer wird gestrichen und *TEL URI* wird durch *GPSI* (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2) ersetzt, da hier nur einige wenige aktuelle Beispiele erscheinen sollen. Das heisst aber nicht, dass Telefonnummer und *TEL URI* nicht mehr als Anfragekriterien verwendet werden können. In *Buchstabe b und c* werden neue Identifikatoren des 5G-Systems eingefügt: SUPI und PEI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10 bzw. Art. 36 Abs. 1 Bst. b Ziff. 4). *Buchstaben d* und *e* bleiben unverändert. In *Buchstabe f* wird die SIM-Nummer (ICCID) als Anfragekriterien hinzugefügt (s. Erläuterungen zur analogen Änderung in Art. 36 Abs. 2 Bst. e).

Art. 42 Abs. 1 Bst. c Einleitungssatz und Ziff. 6 und Bst. d, Abs. 2 Einleitungssatz, Bst. g und j sowie Abs. 3

Wie auch bei den übrigen Auskunftstypen über Kommunikationsdienste (Art. 35, 40 und 43) wird hier in *Absatz 1 Buchstabe c Ziffer 6* ein Feld für die Übermittlung der Bezeichnung des Dienstes hinzugefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 13). In *Buchstabe d* wird ein neuer Identifikator des 5G-Systems (GPSI) eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2).

In *Absatz 2 Buchstabe g* wird bei der UID präzisiert, dass es sich um einen nationalen Identifikator handelt und neu kann die Anfrage auch mit dem LEI (s. Erläuterungen zu Art. 20*b* Abs. 1 Bst. b) gestellt werden. In *Buchstabe j* wird neu der mit dem angefragten Dienst verbundene Identifikator vorgesehen. Es handelt sich hier zum Beispiel

um ein Wiederherstellungs-Adressierungselement wie die E-Mail-Adresse oder die Telefonnummer.

Absatz 3 entspricht dem dritten Satz des bisherigen Absatzes 2.

Art. 43 Abs. 1 und Bst. c Einleitungssätze und Ziff. 6, Abs. 2 Einleitungssatz Bst. g, i und j sowie Abs. 3

In *Absatz 1* werden die Cloud-Dienste gestrichen, da dieser Begriff zu ungenau ist. Als Cloud-Dienste können alle möglichen Arten von Dienstleistungen angeboten werden, darunter auch Dienste, die weder Fernmeldedienste noch abgeleitete Kommunikationsdienste sind (bspw. Computerberechnungen, Übersetzungsdienste). Aus dem gleichen Grund werden auch die Proxy-Dienste gestrichen.

Wie auch bei den übrigen Auskunftstypen über Kommunikationsdienste (Art. 35, 40 und 42) wird hier in *Absatz 1 Buchstabe c Ziffer 6* ein Feld für die Übermittlung der Bezeichnung des Dienstes hinzugefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 13).

In *Absatz 2 Buchstabe g* wird die Möglichkeit der Anfrage mit dem LEI (s. Erläuterungen zu Art. 20*b* Abs. 1 Bst. b) hinzugefügt.

In *Buchstabe i* wird präzisiert, dass es sich um ein Adressierungselement oder einen Identifikator des angefragten Dienstes (Fernmeldedienst oder abgeleiteter Kommunikationsdienst) handelt. Das Auskunftsgesuch kann beispielsweise einen bestimmten eindeutigen applikationsspezifischen Identifikator betreffen, der hier anzugeben ist. Dieser wird für Benachrichtigungen einer App benutzt. Mit diesem Identifikator wird sichergestellt, dass die Benachrichtigung des betreffenden Dienstes an eine bestimmte App auf einem bestimmten Gerät geschickt werden kann (z. B. Device Token des Apple Push Notification Service, Registration Identifier des Google Cloud Messaging, Channel URI des Windows Push Notification Service).

In *Buchstabe j* wird neu der mit dem angefragten Dienst verbundene Identifikator vorgesehen. Es handelt sich hier zum Beispiel um ein Wiederherstellungs-Adressierungselement wie die E-Mail-Adresse oder die Telefonnummer.

Absatz 3 ist inhaltlich unverändert und entspricht dem dritten und vierten Satz des bisherigen Absatzes 2.

Art. 44 Abs. 1 Abs. 1, Einleitungssatz (betrifft nur den italienischen Text), Bst. c und f sowie Abs. 3, Einleitungssatz (betrifft nur den italienischen Text), Bst. c, d und f

In *Absatz 1 Buchstabe c und f* sowie in *Absatz 3 Buchstabe c und d* werden redaktionelle Änderungen im Sinne der geschlechtergerechten Sprache vorgenommen («der oder dem Teilnehmenden» bzw. «der oder des Teilnehmenden»). Inhaltlich ändert sich nichts.

Absatz 3 Buchstabe f wird neu hinzugefügt, um die Anfrage mit einem Code zum Aufladen des Guthabens oder zur Bezahlung der Dienstleistung, wie er üblicherweise für vorbezahlte Dienste (Prepaid) verwendet wird, stellen zu können. Dabei handelt es

sich um einen Code, den man beispielsweise am Kiosk oder an der Kasse eines Supermarktes als Rubbelkarte oder als Kassenzettel kaufen kann. Durch Eingabe des Codes kann man den entsprechenden Betrag auf ein Prepaid-Konto gutschreiben lassen. Bisher gab es im ETSI-Standard noch kein Datenfeld, um diesen Code als Anfragekriterium für ein Auskunftsgesuch verwenden zu können. Da diese Auskunftsmöglichkeit bereits nach der alten VÜPF vom 31. Oktober 2001 bestand, hat der Dienst ÜPF einen entsprechenden Change Request an das ETSI gestellt, der inzwischen angenommen und im Standard hinzugefügt wurde. Somit können die entsprechenden Anfragen neu im standardisierten Verfahren durchgeführt werden.

Art. 45 Auskunftstyp IR_18_ID: Identitätsnachweis

Dieser Artikel wird in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. *Absatz 1* wird an den in Artikel 20*a* verwendeten Begriff «Dokument» (statt «Ausweis») angepasst und geschlechtergerecht formuliert.

In *Absatz 2* wird ein neuer Identifikator des 5G-Systems (SUPI) eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10). Der Rest des Absatzes bleibt inhaltlich unverändert. Die Abkürzung *ICCID* ist im Anhang erklärt. Die Abfragemöglichkeit anhand der Gerätenummer (eingeschränkt mit «gegebenenfalls») steht nur zur Verfügung, wenn die Anbieterin das Gerät abgegeben und die Gerätenummer auch erfasst hat, was bei Mobilfunkdiensten in der Regel nicht der Fall ist.

Art. 46 Abs. 1

Dieser Absatz wird neu geschlechtergerecht («der oder des Teilnehmenden») formuliert.

Art. 47 Auskunftstyp IR_20_CONTRACT: Vertragskopie

Absatz 1 wird neu geschlechtergerecht («der oder de*s* Teilnehmenden») formuliert.

In *Absatz 2* wird ein neuer Identifikator des 5G-Systems (SUPI) eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10). Der Rest des Absatzes bleibt inhaltlich unverändert. Die Abkürzung *ICCID* ist im Anhang erklärt. Die Abfragemöglichkeit anhand der Gerätenummer (eingeschränkt mit «gegebenenfalls») steht nur zur Verfügung, wenn die Anbieterin das Gerät abgegeben und die Gerätenummer auch erfasst hat, was bei Mobilfunkdiensten in der Regel nicht der Fall ist.

Art. 48 Auskunftstyp IR_21_TECH: Technische Daten

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. *Absatz 1* hält fest, dass sich dieses Auskunftsgesuch auf die «am angefragten Standort» vorhandenen Netzelemente bezieht. Weiter wird präzisiert, dass nur diejenigen öffentlichen WLAN-Zugänge betroffen sind, die «professionell betrieben» werden. Der Begriff «WLAN-Zugangspunkt» wird durch den allgemeineren Begriff «WLAN-Zugang» ersetzt (s. Erläuterungen zum *Ersatz von Ausdrücken*, Abs. 1 am Anfang der Verordnung).

In *Absatz 2 Buchstabe a* wird neu der allgemeine Begriff der Zell- oder Gebietsidentifikatoren verwendet, statt beispielhaft die einzelnen Identifikatoren aufzuzählen. Der neue Oberbegriff Zellidentifikator schliesst namentlich die bisherigen Beispiele CGI (2G und 3G), ECGI (4G) und NCGI[23] (5G) ein. Die drei Beispiele für eine Area Identity (SAI[24], RAI[25] und TAI[26]) werden neu unter dem Oberbegriff Gebietsidentifikator zusammengefasst. Diese redaktionellen Änderungen haben jedoch keinen Einfluss auf die Lieferung der bisherigen CGI, ECGI, SAI, RAI und TAI. Soweit technisch zutreffend, sind diese wie bisher zu liefern.

In der Praxis hat sich gezeigt, dass die Identifikation eines bestimmten WLAN-Zugangs oft nicht auf Ebene des Zugangspunkts (*access point*) möglich ist, sondern nur auf Ebene des Hotspots. Daher wird als Alternative zu den Identifikatoren der Netzelemente eine andere geeignete Bezeichnung (z. B. Hotspotname, als Alternative zur BSSID) hinzugefügt, obwohl es sich dabei nicht um einen eindeutigen Identifikator handelt (s. auch Art. 48 Abs. 3 Bst. b, Art. 54 Abs. 3 Bst. a, Art. 56 Abs. 2 Bst. e Ziff. 9, Art. 60 Bst. h, Art. 61 Bst. i Ziff. 4, Art. 64 Abs. 2 und Art. 65 Abs. 3). Die Anbieterin des Hotspots kann den Namen des Hotspots frei wählen. Daher ist der Hotspotname nicht eindeutig, oft nicht selbsterklärend und lässt nicht auf die Anbieterin schliessen. Die Anbieterinnen von öffentlichen Hotspots stellen daher den Behörden eine geeignete Identifikationsmöglichkeit für ihre Hotspots zur Verfügung, zum Beispiel über eine generische Webseite (URL), die man aufrufen kann, wenn man mit dem Hotspot verbunden ist, und somit Angaben über die Hotspot-Anbieterin bekommt. Falls der Hotspotname nicht klar genug ist, das heisst den Hotspot vor Ort nicht unverwechselbar bezeichnet, können andere ausreichend genaue Bezeichnungen verwendet werden, zum Beispiel eine kurze Standortbezeichnung. Diese Änderung bedeutet jedoch nicht, dass die BSSID[27] nicht geliefert werden müsste. Falls die BSSID bekannt ist, muss sie geliefert werden. Die *Buchstaben b, c* und *d* bleiben praktisch unverändert.

Buchstabe e wird hinzugefügt, da in 5G-Mobilfunknetzen Standortangaben der Netzelemente (z. B. Mobilfunkzellen) mit Zeitstempeln versehen werden können.

In *Absatz 3 Buchstabe a* wird durch Hinzufügen des Wortes «angefragten» vor «Standort» präzisiert, dass die Anfrage anhand der Koordinaten eines Standorts gemacht werden kann, das heisst, dass sich die Anfrage auf alle an diesem Standort be-

23 **NCGI** (New Radio Cell Global Identity): unveränderter Identifikator für eine Zelle in Mobilfunknetzen der fünften Generation (5G), gemäss 3GPP TS 23.003, Clause 19.6A. Der NCGI besteht aus der Verkettung des PLMN-Identifikators (MCC + MNC) sowie der NR Cell Identity (NCI) und ist weltweit eindeutig.

24 **SAI** (Service Area Identity): unveränderter Identifikator für ein Dienstabdeckungsgebiet (Service Area), welcher in Mobilfunknetzen für das Mobility Management verwendet wird (s. 3GPP TS 23.003, Clause 12.5)

25 **RAI** (Routing Area Identity): unveränderter Identifikator für ein Routing-Gebiet (Routing Area), welcher in Mobilfunknetzen im Bereich paketvermittelte Datenübertragung für das Mobility Management verwendet wird (s. 3GPP TS 23.003, Clause 4.2)

26 **TAI** (Tracking Area Identity): unveränderter Identifikator für ein Tracking-Gebiet (Tracking Area), welcher in Mobilfunknetzen der vierten Generation für das Mobility Management verwendet wird (s. 3GPP TS 23.003, Clause 19.4.2.3)

27 **BSSID** (Basic Service Set Identifier): eindeutiger Identifikator (MAC-Adresse) des WLAN-Zugangs.

findlichen Netzelemente der MWP bezieht. Gezielte Anfragen nach einem bestimmten Netzelement an diesem Standort sind nach *Buchstabe b* ebenfalls möglich. Dort wird hinzugefügt, dass in der Anfrage zu einem bestimmten Netzelement statt einem standardisierten Identifikator auch eine andere geeignete Bezeichnung (z. B. Hotspotname) verwendet werden kann. Ausserdem wird wie in Absatz 2 Buchstabe a der Oberbegriff Zell- oder Gebietsidentifikator verwendet (s. oben).

Art. 48a Auskunftstyp IR_51_ASSOC_PERM: Auskünfte über längerfristig zugeordnete Identifikatoren

Bei der Erbringung von Fernmeldediensten des IMS können statt der permanenten Dienst- und Geräteidentifikatoren auch längerfristig zugeordnete Identifikatoren ersatzweise verwendet werden. Daher wird dieser neue Auskunftstyp geschaffen, um die zu einem Identifikator längerfristig zugeordneten Identifikatoren abfragen zu können (private IMPI zu öffentlichem IMPU und umgekehrt). Da es sich um Angaben zum Zweck der Identifikation nach Artikel 22 BÜPF handelt, haben die FDA und die AAKD mit weitergehenden Pflichten gemäss Artikel 22 oder 52 diese Daten während der Dauer der Kundenbeziehung sowie während 6 Monaten nach deren Beendigung aufzubewahren und zu liefern (Art. 21 Abs. 1).

Art. 48b Auskunftstyp IR_52_ASSOC_TEMP: sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren

Nach *Absatz 1* können bei der Erbringung von 5G-Mobilfunkdiensten statt der permanenten Dienst- und Geräteidentifikatoren auch kurzzeitig zugeordnete (temporäre) Identifikatoren ersatzweise verwendet werden. Dieser neue Auskunftstyp wird geschaffen, um die zu einem temporären Identifikator zugeordneten permanenten Identifikatoren echtzeitnah abfragen zu können. Das bedeutet, dass die Beantwortung in der Regel in Sekundenbruchteilen erfolgen muss. Eine Aufbewahrung dieser Zuordnungsdaten ist nicht erforderlich.

Absatz 2 regelt die Angaben, welche in der Anfrage enthalten sein müssen. Da die betreffenden temporären Identifikatoren nur innerhalb eines bestimmten Mobilfunkgebietes eindeutig zugeordnet werden können, ist dessen Präzisierung zwingend. Die technischen Details werden im Einzelnen im Annex 1 der VD-ÜPF definiert.

Für die 5G-Technologie ist das folgende Beispiel ein wichtiger Anwendungsfall: Eine berechtigte Behörde erfasst im Rahmen eines Einsatzes besonderer technischer Geräte gemäss Artikel 269bis StPO mit ihren funktechnischen Geräten (z. B. False Base Station) einen temporären Identifikator (z. B. 5G-GUTI oder SUCI). Daraufhin macht sie eine Abfrage gemäss diesem neuen Auskunftstyp, um sofort den zugehörigen permanenten Identifikator (z. B. SUPI) zu erhalten.

Die Antwortzeit dieses neuen Auskunftstyps muss sehr kurz sein (echtzeitnah), weil sich die temporären Identifikatoren oft ändern. Diese Auskunft muss daher automatisiert über eine neue Abfrageschnittstelle abgefragt und erteilt werden. Mit einem Auskunftsgesuch dürfen auch mehrere Identifikatoren gleichzeitig abgefragt werden. Ein massgeblicher Zeitpunkt kann nicht angegeben werden, da es eine echtzeitnahe Ab-

frage ist. Es gilt der Zeitpunkt der Abfrage zuzüglich ein kurzes technisches Toleranzintervall. Abfragen darüber hinaus in die Vergangenheit oder Zukunft sind nicht möglich.

Art. 48c Auskunftstyp IR_53_TEL_ADJ_NET: Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten

Dieser Auskunftstyp wird neu geschaffen, um spezifische Probleme der Identifikation der Täterschaft zu lösen, wie sie bei gefälschter (Spoofing) oder unbekannter Telefonnummer des Anrufers oder Absenders der Mitteilung auftreten. Dies kann zum Beispiel bei anonymen Bombendrohungen nützlich sein, um die Spur des anonymen Anrufs oder der anonymen Mitteilung nachverfolgen zu können.

Die historischen Randdaten (HD) von Verbindungen und Verbindungsversuchen, die zum Zweck der rückwirkenden Überwachung aufbewahrt werden, enthalten die Adressierungselemente der an der Kommunikation Beteiligten (wer mit wem). Wenn die Herkunftsnummer oder die Absenderadresse jedoch gefälscht oder nicht bekannt ist, benötigen die berechtigten Behörden ein Mittel, um den Anruf oder die Mitteilung zurückverfolgen zu können.

Absatz 1 schreibt die zu liefernden Angaben vor. Die Anbieterin muss die Bezeichnung des ihr auf dem Kommunikationspfad unmittelbar benachbarten Netzes «von» und die Bezeichnung des ihr unmittelbar benachbarten Netzes «nach», soweit sie an der angefragten Kommunikation oder dem Kommunikationsversuch beteiligt waren, liefern. Sie muss insbesondere keine Angaben über allfällige weitere, vor- oder nachgelagerte Netze einer Verbindung liefern. Angenommen, es fand ein Anruf statt vom Netz der Anbieterin A über das Netz der Transitanbieterin B zum Netz der Anbieterin C; wenn Transitanbieterin B die Anfrage erhält, muss sie die Anbieterinnen A («von») und C («nach») als benachbarte Netze dieses Anrufs angeben. Wenn Anbieterin A die Anfrage erhält, muss sie die Anbieterin B («nach») angeben (es existiert kein «von»). Wenn Anbieterin C die Anfrage erhält, muss sie die Anbieterin B («von») angeben (es existiert kein «nach»). Es genügt, wenn die Anbieterin ihre üblichen internen Bezeichnungen liefert, beispielsweise einen «Inter Operator Identifier», der eine bestimmte Anbieterin bezeichnet, oder die IP-Adresse des benachbarten Netzes.

Absatz 2 regelt die in der Anfrage anzugebenden Kriterien, damit die fragliche Kommunikation oder der Kommunikationsversuch eindeutig bestimmt werden kann.

Mit diesem Auskunftstyp wird für FDA mit vollen Pflichten und für AAKD mit weitergehenden Überwachungspflichten (Art. 52) eine Aufbewahrungspflicht von 6 Monaten für die entsprechenden Randdaten geschaffen (s. auch Art. 21 Abs. 5 Bst. c und Art. 61 Bst. j). Da jede Anbieterin nur ihre eigenen Netzschnittstellen kontrollieren kann und um verlässliche Angaben zu erhalten, werden nur die Angaben über die an der angefragten Kommunikation oder dem Kommunikationsversuch beteiligten unmittelbar benachbarten Netze verlangt. Die berechtigte Behörde kann auf diese Weise die fragliche Kommunikation durch Anfragen an die einzelnen Anbieterinnen zurück- oder weiterverfolgen.

Dieser neue Auskunftstyp schafft ein standardisiertes Verfahren für die Rückverfolgung respektive Weiterverfolgung von Kommunikationen und Kommunikationsversuchen. Die Bearbeitungszeiten sind im Artikel 14 VD-ÜPF geregelt.

Art. 50 Abs. 1 und 5-9

Analog zu Artikel 18 (Pflichten für die Lieferung von Auskünften) wird *Absatz 1* erweitert, um die Pflichten für die Ausführung der neuen Überwachungstypen gemäss den Artikeln 56*a*, 56*b*, 67 Buchstaben b und c sowie 68 Absatz 1 Buchstaben b und c zu präzisieren. Der *zweite Satz* regelt, dass die AAKD mit weitergehenden Überwachungspflichten (Art. 52) davon befreit sind. Ob diese Überwachungen zukünftig gegebenenfalls auch durch die AAKD durchgeführt werden müssen, wird im Rahmen der zweiten Revision entschieden, wenn die nähere Umschreibung der Kategorien FDA und AAKD umgesetzt wird. Es wird daher vorliegend davon abgesehen, den AAKD neue Pflichten im Zusammenhang mit diesen neuen Überwachungstypen aufzuerlegen.

Absatz 5 wird so angepasst, dass die MWP ihre Unterstützung auf Aufforderung des Dienstes ÜPF zur Verfügung stellen muss (statt «wenn nötig»).

Absatz 6 regelt die Handhabung von zugehörigen Identifikatoren zu Beginn der Überwachung, Notsuche oder Positionsbestimmung, wogegen Absatz 9 die Änderung und das Hinzukommen von zugehörigen Identifikatoren während einer aktiven Echtzeitüberwachung oder periodischen Positionsbestimmung behandelt. Bei Mobilfunkdiensten mit Extra-SIM-Karten (z. B. Multi-Device oder Multi-SIM für zusätzliche Geräte wie Smartphone, Tablet, Smartwatch) sind standardmässig alle Endgeräte, Nummern oder SIM zu überwachen, die zum Targetidentifikator dazugehören (z. B. bei einer Hauptnummer alle Nebennummern). Dies gilt für alle Arten von Überwachungen (Echtzeit, rückwirkend, Positionsbestimmung, Notsuche, Fahndung). Wenn beispielsweise die MSISDN oder die IMSI eines Abonnements überwacht wird, müssen alle Haupt- und Nebennummern dieses Abos überwacht werden und damit auch alle zugehörigen Geräte wie zum Beispiel Smartwatches, die die zugehörigen Telefonnummern oder SIM dieses Abos benutzen. Ausgenommen sind Neben-Targetidentifikatoren, mit denen nicht kommuniziert werden kann (Bsp. technische Nummern) und andere Gerätenummern, wenn der Targetidentifikator selbst eine Gerätenummer ist (d.h. wenn Gerätenummer x überwacht wird, müssen andere Gerätenummern, die eventuell indirekt über das benutzte Abonnement damit in Zusammenhang stehen, nicht überwacht werden. Pro zusätzlichem Endgerät, zusätzlicher Nummer oder SIM wird keine zusätzliche Gebühr fällig und keine zusätzliche Entschädigung ausgerichtet. Bei Bedarf kann die Anbieterin für die Einrichtung der entsprechenden Überwachungen zusätzliche administrative Identifikationsnummern der Überwachung (LIID: Lawful Interception Identifier) beim Dienst ÜPF anfordern. Falls diese gesamthafte Überwachung aller zum Haupt-Targetidentifikator zugehörigen Endgeräte, Nummern oder SIM von der anordnenden Behörde nicht gewünscht wird, ist dies explizit in der Anordnung zu vermerken.

In *Absatz 7* werden die Pflichten bei der Echtzeitüberwachung von Mobilfunkdiensten um die Überwachung der technischen Teilnehmerdatenbanken wie HLR[28], HSS[29] und UDM[30] erweitert, zum Zwecke der Erfassung und Lieferung wichtiger Randdaten des Targets. Diese enthalten insbesondere Informationen über das diensterbringende Netz, über die Änderung der zugeordneten Dienst- und Geräteidentifikatoren, über standortbezogene Ereignisse, über den Wechsel des diensterbringenden Netzelements sowie über Identifizierungs- und Authentifizierungsereignisse.

Absatz 8 sieht vor, dass im IMS die netzwerkseitige Bestimmung (network provided) der Standortangaben des Targets während der Echtzeitüberwachung gegebenenfalls angestossen werden muss.

In *Absatz 9* wird geregelt, dass Änderungen und das Hinzufügen von Multi-Device-Endgeräten, Nummern und SIM, die zum überwachten Dienst gehören, durch die MWP zu beobachten sind. Die MWP hat die Überwachung selbständig an die Veränderungen anzupassen und gegebenenfalls auf die neuen Target-Identifikatoren auszuweiten. Dieser Zusatzaufwand der MWP wird nicht entschädigt. Auch der Dienst ÜPF kann für solche Zusatzaufwendungen keine zusätzliche Gebühr verlangen. Bei Bedarf kann die Anbieterin für das Einrichten weiterer notwendiger Überwachungen zusätzliche LIID (s. Erläuterungen zu Abs. 6) anfordern.

Art. 53 Zugang zu den Anlagen

In *Absatz 1* wird präzisiert, dass auch bei MWP, die lediglich Duldungspflichten haben, die Durchführung von notwendigen Testschaltungen möglich ist. Die Testschaltungen sind in Artikel 30 geregelt. Eine Testschaltung ist insbesondere dann notwendig, wenn eine angeordnete Überwachung vorzubereiten ist oder um die Qualitätskontrolle einer laufenden Überwachung sicherzustellen, auch wenn diese vom Dienst ÜPF technisch umgesetzt wird.

Absatz 2 ist bis auf eine redaktionelle Anpassung im zweiten Satz («Im Einvernehmen mit» statt « in Absprache mit») identisch mit dem bisherigen Absatz 2.

Art. 54 Überwachungstyp RT_22_NA_IRI: Echtzeitüberwachung von Randdaten bei Netzzugangsdiensten

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. Mit der 5G-Technologie sind neu Mehrfachanmeldungen im Netz (multiple registrations) respektive Mehrfachanbindungen (multiple attachments) im gleichen oder in verschiedenen diensterbringenden Netzwerken möglich, was auch einen Wechsel des Ziels

28 **HLR** (Home Location Register): in Mobilfunknetzen der 2. und 3. Generation, Datenbank einer Mobilfunkanbieterin, wo die Funktionsmerkmale ihrer Teilnehmenden (z. B. IMSI, MSISDN, Konfiguration, Dienstprofile) und deren jeweils aktuelles diensterbringendes Netz gespeichert sind.

29 **HSS** (Home Subscriber Server): in Mobilfunknetzen der 4. Generation, ähnliche Funktionen wie HLR.

30 **UDM** (Unified Data Management): in Mobilfunknetzen der 5. Generation, ähnliche Funktionen wie HLR und HSS.

der Überwachung (Target) zwischen den verschiedenen Netzwerken und Technologien ermöglicht[31].

Absatz 1 bleibt unverändert.

Absatz 2 Buchstabe a wird ergänzt, damit die Behörden im Rahmen der Echtzeitüberwachung neu über die Technologie, die ein Target nutzt, und auch über einen Netzwerk- oder Technologiewechsel durch das Target informiert werden. Bei Mobilfunk sind auch die Informationen über die jeweiligen Prozeduren für die Herstellung und Trennung des Netzzugangs gemäss der verwendeten Technologie (wie GPRS, EPS, 5GS) zu übertragen: insbesondere bei GPRS die Ereignisse GPRS Attach, GPRS Detach, PDP Context Activation und PDP Context Deactivation; bei EPS die Ereignisse E-UTRAN Attach, E-UTRAN Detach, Bearer Activation und Bearer Deactivation; bei 5GS die Ereignisse Registration, Deregistration, PDU Session Establishment und PDU Session Release.

Buchstaben b bleibt unverändert.

In *Buchstaben c* und *e* entfällt das redundante «bei Mobilfunk», da der gesamte Artikel nur den Mobilfunk betrifft.

In *Buchstaben c, e* und *f* werden neue Identifikatoren des 5G-Systems (SUPI, GPSI, PEI) eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2 «GPSI» und Ziff. 10 «SUPI» sowie zu Art. 36 Abs. 1 Bst. bZiff. 4 «PEI»).

In *Buchstabe d* dient der Zusatz «zugehörige Endgeräte» zur Präzisierung, dass auch die zugeteilten IP-Adressen von Multi-Device-Geräten zu liefern sind. Ausserdem entfällt die bisherige Erwähnung von IP-Adressbereichen, die hier nicht zutreffend ist.

In *Buchstabe g* wird entsprechend präzisiert, dass es um Ereignisse geht, die die technischen Eigenschaften des überwachten Netzzugangsdienstes oder dessen Mobility Management ändern. Zur Änderung der technischen Eigenschaften gehören zum Beispiel:

- Änderungen der Dienstunterstützung (service support);
- Änderungen des PDP Context, des Bearer oder der PDU Session;
- NAS Signalling Messages des Targets;
- die Aktualisierung der Position des Targets, zum Beispiel Location Update und Mobility Registration Update.

NAS Signalling Messages sind Signalisierungsnachrichten, die über die NAS-Schnittstelle (NAS = Non-Access Stratum) zwischen dem Endgerät und dem Mobilfunk-Kernnetz ausgetauscht werden. Zum Mobility Management gehören zum Beispiel GMM, EMM und Mobility Registration.

In *Buchstabe h* werden eine redaktionelle Angleichung an den Wortlaut des Artikels 56 Absatz 2 Buchstabe e Ziffer 9 und eine Begriffsbereinigung vorgenommen, indem «momentan» durch «aktuell» ersetzt wird. Ausserdem wird neu aufgenommen, dass die aktuellen Standortangaben soweit wie möglich vom Netzwerk zu bestimmen

[31] Vgl. dazu 3GPP TS 33.501 Abschnitt 6.3.2.

und dementsprechend zu kennzeichnen sind. Vom Netzwerk bestimmte Standortangaben sind vertrauenswürdiger als solche, die vom Endgerät bestimmt werden. Vom Endgerät bestimmte Standortangaben können nämlich gefälscht sein. Es sind jedoch alle vorhandenen Standortangaben zu liefern, auch die vom Endgerät bestimmten, welche entsprechend zu kennzeichnen sind. Die Kennzeichnung mit dem Attribut «vom Netzwerk bestimmt» oder «vom Endgerät bestimmt» hilft den Behörden bei der Einschätzung, inwiefern sie den Standortangaben vertrauen können. Neu hinzugefügt wird die Vorschrift, dass auch die das Target betreffenden Standortangaben aus NAS-Signalisierungs-Nachrichten zu übermitteln sind. Bei den Mobilfunksystemen der 4. Generation (EPS) und der 5. Generation (5GS) können im System Zeitstempel und Altersangaben zu den Standortangaben verfügbar sein; sie sind dementsprechend ebenfalls zu übermitteln. Unter «Alter der Standortangabe» ist die Zeitspanne zu verstehen, die zwischen der tatsächlichen Bestimmung der Standortangabe und der Übermittlung dieser Information vergangen ist.

In den *Buchstaben i–k* wird die Lieferung wichtiger Randdaten geregelt, die bei der Überwachung von technischen Teilnehmerdatenbanken wie HLR, HSS und UDM (s. Erläuterungen zu Art. 50 Abs. 7) erfasst werden können.

In *Buchstabe i* handelt es sich um Informationen über das vorherige und das aktuelle diensterbringende Netz, das heisst Ereignisse vom Typ «Serving System» (*diensterbringendes Netz*, z. B. Serving PLMN, VPLMN ID).

In *Buchstabe j* handelt es sich um:

- Informationen über die Änderung der zugeordneten Dienst- und Geräteidentifikatoren (z. B. IMSI, MSISDN, IMEI, SIP-URI, IMPI), das heisst Ereignisse vom Typ Susbcriber Record Change. Es sind insbesondere auch temporäre Identifikatoren zu übermitteln, auch wenn deren Lebensdauer nur kurz ist.
- Informationen über standortbezogene Ereignisse und gegebenenfalls deren Grund (z. B. Ereignisse vom Typ Register Location, Cancel Location, Register Termination).
- Informationen über den Wechsel des diensterbringenden Netzelements (z. B. SGSN, MME, MSC, AMF).
- Informationen über Identifizierungs- und Authentifizierungsereignisse des Targets (z. B. Zugangsberechtigung an einem PWLAN erhalten).

In *Buchstabe k* wird eine Regelung hinzugefügt, die nur die 5G-Technologie betrifft. Es sind zusätzlich Informationen über die Zuordnung von neuen temporären Identifikatoren des Targets zu liefern. Dies betrifft insbesondere das Verschleiern («concealing») von Teilnehmeridentifikatoren (z. B. SUCI statt SUPI). Die temporären Identifikatoren sind jeweils bei Neuzuordnung zu übermitteln, auch wenn deren Lebensdauer nur kurz ist.

In *Absatz 3* wird eine redaktionelle Änderung vorgenommen. Statt dem Begriff «Mobilfunktechnologie» (in den bisherigen Bst. a-c) wird der allgemeinere Begriff «Netzzugangstechnologie» verwendet, da Nicht-3GPP-Zugangstechnologien wie WLAN-Zugang ebenfalls betroffen sind. In *Buchstabe a* wird, analog zu Artikel 48 Absatz 2

Buchstabe a (s. dortige Erläuterungen), der allgemeine Begriff der Zell- oder Gebietsidentifikatoren verwendet. Neu hinzugefügt wird der Fall, wenn das Target einen Funkzellenverbund («*combined cell*», Mobilfunkzelle, die aus mehreren geografisch verteilten Antennen besteht) benutzt. Aufgrund der Komplexität dieser Regelung wird hierbei auf den Anhang 1 der VD-ÜPF verwiesen. Die Standortangaben im Falle von WLAN-Zugang (neu: Nicht-3GPP-Zugang) werden nicht mehr hier, sondern im neuen Buchstaben d geregelt. *Buchstaben b* bleibt inhaltlich unverändert. In *Buchstabe c* entfällt ebenfalls die Standortangabe bei WLAN-Zugang, die nun im neuen Buchstaben d geregelt ist. *Buchstabe d* bestimmt die zu liefernden Standortangaben bei einem Nicht-3GPP-Zugang zum Mobilfunkkernnetz näher. Es gibt zwei Varianten: Ziffer 1 für WLAN-Zugang und Ziffer 2 für Festnetzzugang.

Art. 56 Überwachungstyp RT_24_TEL_IRI: Echtzeitüberwachung von Randdaten bei Telefonie- und Multimediadiensten

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. Der bisherige Absatz 1 wird in zwei Absätze unterteilt.

Absatz 1 entspricht dem bisherigen Absatz 1, erster Satz.

Der Einleitungssatz von *Absatz 2* entspricht dem bisherigen Absatz 1, zweiter Satz. *Buchstabe a* ist unverändert und entspricht dem bisherigen Absatz 1 Buchstabe a. In *Buchstabe b* wird statt «Mobilfunk» der Begriff «Mobilfunkdienste» gebraucht und als Alternative zur IMSI ein neuer Identifikator des 5G-Systems, SUPI, eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10). Der Inhalt des bisherigen Buchstabens b^{bis} wird am Ende von Buchstabe b unverändert angefügt. Die *Buchstaben c* und *d* sind unverändert und entsprechen den bisherigen Buchstaben c und d von Absatz 1 mit einer redaktionellen Anpassung im Sinne der geschlechtergerechten Sprache («der oder des Teilnehmenden») in Buchstabe c.

Buchstabe e enthält redaktionelle Anpassungen zur besseren Lesbarkeit. Der Begriff «Netzzugangstechnologie» ersetzt «Mobilfunktechnologie», da auch der Wechsel des Targets auf einen Nicht-3GPP-Zugang mitzuteilen ist. *Ziffern 1–9* entsprechen den Ziffern des bisherigen Buchstabens e des Absatzes 1 mit den folgenden Änderungen: In *Ziffer 2* wird durch Einfügen des Wortes «jeweils» präzisiert, dass die Rolle jedes Kommunikationsteilnehmenden mitzuteilen ist. Ausserdem wird der 5G-Identifikator GPSI eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2). In Ziffer *4* wird der 5G-Identifikator PEI eingefügt (s. Erläuterungen zu Art. 36 Abs. 1 Bst. b Ziff. 4). In *Ziffer 9* wird die wenig gebräuchliche Bezeichnung «ortsunabhängige Dienste» in «Mobilfunkdienste» geändert. Ausserdem wird neu aufgenommen, dass die Standortangaben des Targets soweit möglich vom Netzwerk zu bestimmen und dementsprechend zu kennzeichnen (vom Netzwerk bestimmt/nicht vom Netzwerk bestimmt) sind (s. Erläuterungen zu Art. 54 Abs. 2 Bst. h). Der Begriff «momentane Standortangaben» wird in «aktuelle Standortangaben» geändert. Für die nähere Umschreibung der Standortangaben wird neu auf Artikel 54 Absatz 3 verwiesen. Der bisherige Absatz 2 entfällt somit. Da das Target auch gleichzeitig mehrere Zellen benutzen kann, wird «benutze Zelle» in den Plural gesetzt. Statt «WLAN-Zugangspunkt» wird neu der universellere Begriff «Nicht-3GPP-Zugang» verwendet. Neu hinzugefügt werden die

Vorschriften, dass auch die das Target betreffenden Standortangaben aus NAS-Signalisierungs-Nachrichten zu übermitteln und bei EPS und 5GS die Standortangaben, soweit verfügbar, mit dem jeweiligen verknüpften Zeitstempel oder dem Alter der Standortangabe zu ergänzen sind (s. Erläuterungen zu Art. 54 Abs. 2 Bst. h).

Neu hinzugefügt wird *Buchstabe f,* der die Lieferung wichtiger Randdaten regelt, die bei der Überwachung von technischen Teilnehmerdatenbanken wie HLR, HSS und UDM erfasst werden können (s. Erläuterungen zu Art. 50 Abs. 7 und zu Art. 54 Abs. 2 Bst i, j und k).

Art. 56a Überwachungstyp RT_54_POS_ONCE: einmalige, sofortige Positionsbestimmung durch das Netzwerk

Die Positionsbestimmung nach BÜPF (LALS, Lawful Access to Location Services) ist eine Funktion im Mobilfunknetz, die neu eingeführt wird. Sie gilt als Überwachung nach Artikel 269 StPO, das heisst es müssen die gleichen strengen Voraussetzungen wie bei einer Echtzeitüberwachung erfüllt sein. In dieser Bestimmung wird der erste Überwachungstyp der neuen Positionsbestimmung mittels LALS geregelt: einmalige («ONCE»), sofortige Positionsbestimmung durch das Netzwerk.

Standort und *Position* haben in dieser Verordnung eine unterschiedliche Bedeutung. Bisher gab es nur Standortangaben («location information», Lokalisierung). Unter *Standort* versteht man den Antennenstandort der diensterbringenden Zelle, soweit möglich angereichert mit weiteren Angaben wie Hauptstrahlrichtung der Antenne. Der Standort ist damit nur eine grobe Näherung des Ortes, wo sich das Target (Endgerät) tatsächlich befindet. Die diensterbringende Zelle ist die Zelle um die Antenne, mit der das Target verbunden ist oder zuletzt verbunden war. Je grösser die Reichweite dieser Antenne ist, umso grösser ist die Abweichung des tatsächlichen Aufenthaltsortes des Targets vom angegebenen Standort. Im ländlichen Raum sind mehr als 30 km Abweichung zwischen dem Antennenstandort und dem tatsächlichen Aufenthaltsort des Targets möglich, in Berggebieten in Extremfällen noch weitaus mehr. Der aktuelle Standort des Targets wird bei Echtzeitüberwachungen fortlaufend mitgeteilt. Bei rückwirkenden Überwachungen sind die Standortangaben zu Beginn und am Ende der Kommunikationen respektive Netzzugangs-Sitzungen enthalten. Ausserdem kann der letzte bekannte Standort des Targets mit einer Notsuche EP_35_PAGING oder mit einer Überwachung HD_31_PAGING einzeln abgefragt werden.

Unter *Position* versteht man dagegen den präzisen Ort, wo sich das Target (Endgerät) im Moment der Positionsbestimmung tatsächlich befindet. Es werden zwei Überwachungstypen der Positionsbestimmung mittels LALS eingeführt:

1) Einmalige, sofortige Positionsbestimmung (der vorliegende Artikel),
2) Periodisch wiederkehrende Positionsbestimmung (s. Art. 56*b*).

Gemäss *Absatz 1* ist die einmalige, sofortige Positionsbestimmung von der Mobilfunkanbieterin mittels einer Positionsbestimmungsfunktion des Netzwerks (LALS) durchzuführen. Dabei sind die Positionen von allen mit dem Target-ID assoziierten mobilen Endgeräten zu bestimmen. Wenn der überwachte Identifikator (Target-ID) eine Gerätenummer ist, betrifft dies nur genau ein Gerät. Wenn aber der überwachte Identifikator (Target-ID) ein Adressierungselement (z. B. MSISDN/GPSI) oder eine

Teilnehmeridentifikationsnummer (z. B. IMSI/SUPI) ist, können mehrere Endgeräte wie Smartphones, Tablets und Smartwatches mit der entsprechenden Subscription (Abonnement oder Prepaid) benutzt werden, insbesondere wenn mehrere SIM dazugehören. Da in der Regel nicht bekannt ist, welches Gerät die überwachte Person gerade auf sich trägt, sind die jeweiligen Positionen aller aktuell zugehörigen Geräte zu bestimmen (s. auch die Erläuterungen zu Art. 50 Abs. 6).

Gemäss *Absatz 2* werden die technischen Ausführungsvorschriften vom EJPD in der VD-ÜPF und ihrem Anhang 1 erlassen. Es liegen bisher noch keine praktischen Erfahrungen mit dieser neuen einmaligen, sofortigen Positionsbestimmung vor. Die Positionsbestimmung kann je nach technischer Implementierung möglicherweise eine gewisse Zeit dauern. Die ermittelten Positionen der Endgeräte sind jedoch von der Mobilfunkanbieterin sofort und verzögerungsfrei zu übermitteln.

In *Absatz 3* werden die zu übermittelnden Angaben näher bestimmt. Die Angaben nach den *Buchstaben a und b* sowie *Buchstabe c Ziffern 1–3* sind obligatorisch. Die weiteren Angaben nach *Buchstabe c Ziffer 4* sind zu übermitteln, soweit sie ermittelt werden können beziehungsweise verfügbar sind.

Gemäss *Buchstabe d* ist bei nicht erfolgreicher Positionsbestimmung der Grund des Misserfolgs (Fehlercode) mitzuteilen. Damit die anordnende Behörde bei einer gescheiterten Positionsbestimmung zumindest die Standortdaten erhält, ist als Fallback-Szenario ein «Paging» im Sinne von Artikel 63 durchzuführen, gestützt auf die vorliegende Anordnung der Positionsbestimmung.

Art. 56b Überwachungstyp RT_55_POS_PERIOD: periodisch wiederkehrende Positionsbestimmung durch das Netzwerk

Die einführenden Bemerkungen zu Artikel 56*a* gelten auch für den vorliegenden Artikel. Hierbei handelt es sich um den zweiten Überwachungstyp der Positionsbestimmung mittels LALS: die periodisch wiederkehrende Positionsbestimmung durch das Netzwerk («PERIOD»).

Gemäss *Absatz 1* ist die periodisch wiederkehrende Positionsbestimmung von der Mobilfunkanbieterin mittels einer Positionsbestimmungsfunktion des Netzwerks (LALS) durchzuführen. Dabei sind die Positionen von allen mit dem Target-ID assoziierten mobilen Endgeräten zu bestimmen (s. die Erläuterungen zu Art. 56*a* Abs. 1).

Die technischen Ausführungsvorschriften werden vom EJPD in der VD-ÜPF und ihrem Anhang 1 erlassen (*Abs. 2*). Das EJPD kann beispielsweise vorsehen, dass die Positionsbestimmung in festen vordefinierten Zeitintervallen erfolgt. Da bisher noch keine praktischen Erfahrungen mit dieser neuen periodisch wiederkehrenden Positionsbestimmung vorliegen, insbesondere hinsichtlich des Ressourcenverbrauchs und des Zeitbedarfs der einzelnen Positionsbestimmungen, können noch keine konkreten Vorgaben hinsichtlich der technischen Parameter wie Häufigkeit, Periodizität und Mindestzeitabstand zwischen zwei aufeinanderfolgenden Positionsbestimmungen gemacht werden. Je nach technischer Implementierung kann die Positionsbestimmung eine gewisse Zeit dauern. Die ermittelten Positionen der Endgeräte sind jedoch von der Mobilfunkanbieterin sofort und verzögerungsfrei zu übermitteln.

Gemäss *Absatz 3 Buchstabe d* ist bei nicht erfolgreicher Positionsbestimmung der Grund des Misserfolgs (Fehlercode) mitzuteilen. Aufgrund der automatisierten Ausführung dieses Überwachungstyps ist nach aktuellem Wissensstand leider kein Fallback-Szenario wie bei Artikel 56*a* möglich.

Art. 60 Überwachungstyp HD_28_NA: rückwirkende Überwachung von Randdaten bei Netzzugangsdiensten

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. Die *Buchstaben a-c* und *j* (bisher i) bleiben materiell unverändert. Buchstabe c wird redaktionell leicht angepasst.

In *Buchstabe d* wird «Adressbereiche» gestrichen. Hier geht es um die zum damaligen Zeitpunkt dem Target tatsächlich zugeteilte IP-Adresse. Neu eingefügt werden die Angaben bei einem Nicht-3GPP-Zugang, da der Zugang zum Mobilfunkkernnetz auch anderweitig als über eine Mobilfunkantenne (3GPP-Zugang) erfolgen kann, zum Beispiel über das WLAN zu Hause oder über ein öffentliches WLAN. Wenn keine Mobilfunkantenne beteiligt ist, entfallen auch deren Standortangaben (Bst. g). Über diese Quell-IP-Adresse und Portnummer ist die Bestimmung des Zugangsstandortes möglich.

In den *Buchstaben e* und *f* wird die Einschränkung «sofern verfügbar» gestrichen, da es sich hier um Pflichtparameter handelt. Ausserdem wird in den *Buchstabe e* und *g* der Begriff «Mobilfunk» zu «Mobilfunkdienst» geändert.

In den *Buchstaben e, g* und *h* werden neue Identifikatoren des 5G-Systems (PEI, SUPI, GPSI) eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2 «GPSI» und Ziff. 10 «SUPI» sowie Art. 36 Abs. 1 Bst. b Ziff. 4 «PEI»).

In *Buchstabe g* werden die mit Standortangaben verknüpften Zeitstempel hinzugefügt, die bei der Mobilfunktechnologie der 4. Generation (EPS) und der 5. Generation (5GS) im System verfügbar sein können. Sie sind dementsprechend ebenfalls zu übermitteln. Die einzelnen Standortangaben werden nicht mehr näher in diesem Buchstaben umschrieben, da sie für dieses Format zu komplex geworden sind. Es wird stattdessen auf die anwendbaren Vorschriften des EJPD verwiesen, die sich im Anhang 1 der VD-ÜPF befinden.

In *Buchstabe h* wird präzisiert, dass diese Regelung nur für öffentliche WLAN-Zugänge gilt, die professionell betrieben werden. Aufgrund der Erfahrungen aus der Praxis wird die Möglichkeit eingefügt, statt eines eindeutigen Identifikators eine andere geeignete Bezeichnung wie «Hotspotname» anzugeben. Es genügt hier eine ausreichend genaue Bezeichnung des WLAN-Zugangs, das heisst die gelieferte Bezeichnung muss den WLAN-Zugang am Ort ausreichend genau bezeichnen (s. Erläuterungen zu Art. 48 Abs. 2 Bst. a).

In *Buchstabe i* wird die Regelung betreffend die Standortinformationen aus der Seeschifffahrt und der Luftfahrt, die sich bisher jeweils am Ende der Buchstaben g und h befand, übernommen und in einem Buchstaben zusammengefasst.

Buchstabe j entspricht dem bisherigen Buchstaben i.

Art. 61, Einleitungssatz, Bst. b, d, g, g^{bis}, i und j

In den *Buchstaben b* und *d* werden neue Identifikatoren des 5G-Systems (PEI, SUPI, GPSI) eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2 «GPSI» und Ziff. 10 «SUPI» sowie Art. 36 Abs. 1 Bst. b Ziff. 4 «PEI»).

In *Buchstabe g* werden die einzelnen Standortangaben nicht mehr näher umschrieben, da sie für dieses Format zu komplex geworden sind. Es wird stattdessen auf die anwendbaren Vorschriften des EJPD verwiesen, die sich im Anhang 1 der VD-ÜPF befinden.

In *Buchstabe g^{bis}* wird, wie in Artikel 60 Buchstabe i, die Regelung betreffend die Standortinformationen aus der Seeschifffahrt und der Luftfahrt übernommen. Diese befand sich am Ende des Einleitungssatzes des bisherigen Buchstabens g.

Buchstabe i bleibt materiell unverändert. In *Ziffer 4* wird auf die anwendbaren Vorschriften des EJPD verwiesen, das heisst auf Anhang 1 VD-ÜPF.

Nach *Buchstabe j* sind nun auch die Angaben über das auf dem Kommunikationspfad unmittelbar benachbarte Netz, also dasjenige woher die Angaben kommen («von») und dasjenige wohin sie gehen («nach»), zu liefern, soweit sie an der Kommunikation oder dem Kommunikationsversuch beteiligt waren. Damit sollen die Strafverfolgungsbehörden im Falle einer unbekannten oder vorgetäuschten Telefonnummer (sog. «Spoofing») die Möglichkeit erhalten, den Kommunikationspfad nachzuverfolgen und damit die entsprechenden Ursprünge der Kommunikation oder des Kommunikationsversuches identifizieren zu können (s. auch Erläuterungen und Beispiel zu Art. 48*c*). Dies kann unter anderem bei anonymen Bombendrohungen nützlich sein, um die Spur des anonymen Anrufs oder der anonymen Mitteilung nachverfolgen zu können. Die historischen Randdaten (HD) von Verbindungen und Verbindungsversuchen, die zum Zweck der rückwirkenden Überwachung aufbewahrt werden, enthalten die Adressierungselemente der an der Kommunikation Beteiligten (wer mit wem). Wenn die Herkunftsnummer jedoch gefälscht oder nicht bekannt ist, benötigen die berechtigten Behörden weitere Angaben, um den Anruf oder die Mitteilung zurück- oder weiterverfolgen zu können.

Da jede Anbieterin nur ihre eigenen Netzschnittstellen kontrollieren kann und um verlässliche Angaben zu erhalten, muss die Anbieterin nur die Angaben über das ihr unmittelbar benachbarte Netz «von» und das ihr unmittelbar benachbarte Netz «nach», soweit sie an der angefragten Kommunikation oder dem Kommunikationsversuch beteiligt waren, aufbewahren. Die Aufbewahrungsdauer dieser Randdaten beträgt 6 Monate (Art. 26 Abs. 5 BÜPF) und betrifft nur die Anbieterinnen mit Überwachungspflichten.

Die Anbieterin muss insbesondere keine Angaben über allfällige weitere, vor- oder nachgelagerte Netze einer Verbindung aufbewahren. Weitere der Anbieterin zur Verfügung stehende Randdaten sind jedoch auf Verlangen zu liefern (Art. 26 Abs. 6, Art. 27 Abs. 2, Art. 28 Abs. 2 und Art. 29 Abs. 2 BÜPF). Solche zusätzlichen Angaben sind nicht Teil dieses standardisierten Überwachungstyps und können als besondere Überwachung nach Artikel 25 VÜPF herausverlangt werden.

Die Übermittlung von Angaben über die unmittelbar benachbarten Netze ist jedoch für die Echtzeitüberwachung schwierig umsetzbar und nicht mit den entsprechenden

Standards von ETSI und 3GPP kompatibel. Daher wird auf eine analoge Bestimmung in Artikel 56 Absatz 2 Buchstabe e verzichtet.

Art. 62 Überwachungstyp HD_30_EMAIL: rückwirkende Überwachung von Randdaten bei E-Mail-Diensten

Dieser Artikel wird in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. In *Buchstabe a* wird als Ergänzung zur IP-Adresse auch die jeweilige Portnummer hinzugefügt, damit die Identifikation dieser Server und Clients im Falle von Network Address Translation (NAT) ermöglicht wird.

Die Speicherpflicht für die Randdaten von E-Mail-Diensten (History) haben nur MWP mit vollen Überwachungspflichten, das heisst FDA mit vollen Pflichten und AAKD mit weitergehenden Überwachungspflichten (Art. 52). Alle anderen MWP liefern lediglich die ihnen zur Verfügung stehenden Daten.

Art. 63 Überwachungstyp HD_31_PAGING: Bestimmung des Standorts bei der letzten Aktivität

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. In *Absatz 1* wird präzisiert, dass es sich nicht um die letzte festgestellte, sondern um die letzte feststellbare Aktivität handelt. Bei Bedarf hat die MWP also den Standort der letzten Aktivität festzustellen. Ausserdem wird der ganze Satz in die Mehrzahl gesetzt, da der Standort der jeweils letzten Aktivität von allen mit dem Target-ID assoziierten Endgeräten (also gegebenenfalls nicht nur von einem) festzustellen ist (s. die Erläuterungen zu Art. 56*a* Abs. 1).

Die zu übermittelnden Angaben werden in *Absatz 2* im Einzelnen geregelt und neu strukturiert. Es kommen jedoch keine neuen Angaben im Vergleich zur bisherigen Version hinzu, mit Ausnahme der neuen äquivalenten Parameter des 5G-Systems, deren Bezeichnungen sich geändert haben (z. B. GPSI für MSISDN, SUPI für IMSI, PEI für IMEI). Weiter wird in *Buchstabe h* auf die anwendbaren Vorschriften des EJPD verwiesen, das heisst auf Anhang 1 VD-ÜPF.

Art. 64 Abs. 2

In *Absatz 2* wird der allgemeine Begriff der Zell- oder Gebietsidentifikatoren (s. Erläuterungen zu Art. 48 Abs. 2 Bst. a) verwendet, statt beispielhaft die einzelnen Identifikatoren aufzuzählen. Weiter wird präzisiert, dass nur öffentliche WLAN-Zugänge betroffen sind, die «professionell betrieben» werden. Ausserdem wird der allgemeinere Begriff «WLAN-Zugang» statt «WLAN-Zugangspunkt» verwendet (s. Erläuterungen zum Ersatz von Ausdrücken, Abs. 1). Statt des Identifikators des WLAN-Zugangs kann auch eine andere geeignete Bezeichnung (z. B. Hotspotname) geliefert werden (s. Erläuterungen zu Art. 48 Abs. 2 Bst. a).

Art. 65 Abs. 2 Einleitungssatz und Abs. 3

In *Absatz 2* wird der Einleitungssatz redaktionell geändert.

In *Absatz 3* wird der allgemeinere Begriff «WLAN-Zugang» statt «WLAN-Zugangspunkt» verwendet (s. Erläuterungen zum Ersatz von Ausdrücken, Abs. 1). Zudem wird der allgemeine Begriff der Zell- oder Gebietsidentifikatoren (s. Erläuterungen zu Art. 48 Abs. 2 Bst. a) verwendet, statt der beispielhaften Aufzählung einzelner Identifikatoren. Statt des Identifikators des WLAN-Zugangs kann auch eine andere geeignete Bezeichnung (z. B. Hotspotname) geliefert werden (s. Erläuterungen zu Art. 48 Abs. 2 Bst. a).

Art. 67 Überwachungstypen EP: Notsuche

Dieser Artikel wird aufgrund der zahlreichen Änderungen in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. Die Bestimmung wird neu strukturiert. Zudem werden zwei neue Echtzeitüberwachungstypen für die Notsuche eingeführt. Die übrigen Typen der Notsuche werden beibehalten.

Es sind die bei Artikel 50 Absatz 6 erläuterten Änderungen bezüglich Mobilfunkdienste mit Extra-SIM-Karten (z. B. Multi-Device oder Multi-SIM für zusätzliche Geräte wie Smartphone, Tablet, Smartwatch) zu beachten.

Buchstabe a definiert wie bisher die Notsuche des Typs «Paging», welcher dem Überwachungstyp HD_31_PAGING entspricht (s. die Erläuterungen zu Art. 63). Neu hinzugekommen ist die Präzisierung, dass auch die jeweiligen Standortangaben bei der letzten Aktivität von allen mit dem Target-ID assoziierten mobilen Endgeräten der vermissten oder einer dritten Person durch die MWP zu bestimmen sind. Diese Präzisierung betrifft vor allem Mobilfunkabonnemente mit Extra-SIM (sog. Multi-Device- oder Multi-SIM-Angebote, s. die Erläuterungen zu Art. 56*a* Abs. 1). Bei diesem bereits seit vielen Jahren existierenden Typ der Notsuche handelt es sich um die Standortbestimmung von mobilen Endgeräten anhand der Mobilfunkzellen. Es ist jeweils der letzte verfügbare Standort des jeweiligen mobilen Endgeräts zu liefern, unabhängig davon, welche Technologie und welcher Netzzugangstyp mit dem Gerät benutzt wurde.

Neu hinzugekommen ist der in *Buchstabe b* definierte Typ EP_56_POS_ONCE, die einmalige, sofortige Positionsbestimmung durch das Netzwerk von allen mit dem Target-ID assoziierten mobilen Endgeräten der vermissten oder einer dritten Person im Rahmen einer Notsuche. Technisch entspricht dieser Typ dem neuen Überwachungstyp RT_54_POS_ONCE (s. auch die Erläuterungen zu Art. 56*a*).

Ebenfalls neu ist der in *Buchstabe c* definierte Typ EP_57_POS_PERIOD, die periodisch wiederkehrende Positionsbestimmung durch das Netzwerk von allen mit dem Target-ID assoziierten mobilen Endgeräten der vermissten oder einer dritten Person im Rahmen einer Notsuche. Technisch entspricht dieser Typ dem neuen Überwachungstyp RT_55_POS_PERIOD (s. auch die Erläuterungen zu Art. 56*b*).

Im Unterschied zur Standortbestimmung nach Buchstabe a ist die Positionsbestimmung nach den Buchstaben b und c weitaus präziser. Sie wird durch spezielle Funktionen des Netzwerks durchgeführt, die einen grösseren technischen Aufwand erfordern. Die neuen Positionsbestimmungsfunktionen erlauben es, genauere Daten über die Position des Mobiltelefons der gesuchten Person zu erhalten. Ungenaue Standortangaben führen zu Zeitverlust bei der Rettung von Personen sowie zu grossem Personal- und Materialeinsatz (wie Polizeiwagen und Helikopter), was

erhebliche Kosten verursacht. Mit einer wesentlich genaueren Lokalisierung der gesuchten Person können Rettungsaktionen gezielter durchgeführt und damit Menschenleben gerettet werden.

Buchstabe d entspricht dem bisherigen Buchstaben b und regelt die Echtzeitüberwachung mit Inhalt und Randdaten im Rahmen einer Notsuche. Die anordnende Behörde erteilt jeweils eine Anordnung pro MWP und pro überwachte Hauptnummer an den Dienst ÜPF, welcher die entsprechenden MWP mit der Notsuche beauftragt. Jede beauftragte MWP richtet die jeweils zutreffenden Überwachungstypen gemäss den Artikeln 55 und 57 ein, so dass alle von ihr erbrachten Dienste der Kategorien TEL und NA für die zur gesuchten Hauptnummer zugehörigen Nebennummern abgedeckt sind. Mit dieser Bündelung wird der Dringlichkeit einer Notsuche Rechnung getragen, da es um das schnellstmögliche Auffinden von Personen geht, die an Leib und Leben bedroht sind. Einzelne Aufträge pro überwachten Telefonie- und Multimediadienst (TEL) oder Netzzugangsdienst (NA), wie sie sonst bei Überwachungen erteilt werden, würden bei einer Notsuche zu viel Zeit kosten. Auch hier sind allfällige zur überwachten Hauptnummer zugehörige Nebennummern ebenfalls zu überwachen (z. B. Abonnements mit Extra-SIM, sog. Multi-Device- oder Multi-SIM-Angebote). Hierzu ein Beispiel: Die MWP erhält einen Auftrag für die Notsuche vom Typ EP_36_RT_CC_IRI (Bst. b) für die MSISDN x. Angenommen, der Teilnehmende mit der MSISDN x hat bei der MWP ein Mobilabonnement mit Telefonie- und Internetzugang, welches eine Extra-SIM mit der MSISDN y für den Internetzugang enthält, dann richtet die MWP entsprechend für den Telefoniedienst eine Echtzeitüberwachung von Inhalten und Randdaten bei Telefonie- und Multimediadiensten (Art. 57) für die MSISDN x und für den Netzzugang eine Echtzeitüberwachung von Inhalten und Randdaten bei Netzzugangsdiensten (Art. 55) für die MSISDN x sowie eine weitere für die MSISDN y ein. Die Echtzeitüberwachungen bleiben auch im Rahmen einer Notsuche so lange aktiv, bis der Dienst ÜPF die jeweiligen Aufhebungsaufträge an die entsprechenden MWP erteilt.

Buchstabe e entspricht dem bisherigen Buchstaben c und definiert die Echtzeitüberwachung ohne Inhaltsdaten, das heisst nur der Randdaten, im Rahmen einer Notsuche. Das Vorgehen ist entsprechend wie unter Buchstabe d erläutert, mit dem Unterschied, dass sich dieser Überwachungstyp auf die Überwachungstypen gemäss den Artikeln 54 und 56 stützt.

Buchstabe f regelt die rückwirkende Notsuche beispielsweise für den Fall, dass ein Endgerät nicht mehr eingeschaltet ist oder keine Netzabdeckung hat und daher keine aktuellen Daten zur Verfügung stehen. Das Vorgehen ist entsprechend wie unter Buchstabe d erläutert. Die Unterschiede zu Buchstabe d bestehen darin, dass es sich um rückwirkende Überwachungen handelt und dass jede beauftragte MWP die jeweils zutreffenden Überwachungstypen gemäss den Artikeln 60 und 61 einrichtet, so dass alle von ihr erbrachten Dienste für die überwachte Nummer und die mit dieser assoziierten Nummern abgedeckt sind (s. die Erläuterungen zu Art. 50 Abs. 6). Es gelten die üblichen Regeln für rückwirkende Überwachungen (keine Aufhebungsaufträge, Beginn und Ende gemäss Art. 4*a*). Die Entschädigung für die MWP richtet sich nach der Anzahl der durch die Behörden angeordneten Notsuchen

pro MWP und pro beauftragte Nummer und nicht nach der Anzahl der letztlich durchgeführten Überwachungen.

In verschiedenen Bestimmungen werden neue Identifikatoren des 5G-Systems (GPSI, SUPI, PEI) eingefügt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2 «GPSI» und Ziff. 10 «SUPI» sowie Art. 36 Abs. 1 Bst. b Ziff. 4 «PEI»).

Art. 68 Fahndung

Dieser Artikel wird in seiner Gesamtheit revidiert, um die Lesbarkeit zu verbessern und die Verständlichkeit zu erhöhen. Bei der Fahndung kommen drei neue Typen in den *Buchstaben a–c* hinzu.

Buchstabe a führt neu das sogenannte «Paging» im Rahmen einer Fahndung ein, also die Bestimmung des Standorts bei der letzten Aktivität nach Artikel 63 (s. die dortigen Erläuterungen).

Buchstabe b führt neu das einmalige LALS im Rahmen einer Fahndung ein, also die einmalige, sofortige Positionsbestimmung durch das Netzwerk nach Artikel 56*a* (s. die dortigen Erläuterungen).

Buchstabe c führt neu das periodisch wiederkehrende LALS im Rahmen einer Fahndung ein, also die periodisch wiederkehrende Positionsbestimmung durch das Netzwerk nach Artikel 56*b* (s. die dortigen Erläuterungen).

Die übrigen Buchstaben bleiben unverändert. Sie verschieben sich lediglich nach hinten (aus *Bst. a* wird *Bst. d*, … und aus *Bst. d* wird *Bst. g*).

In *Absatz 2* wird bezüglich Beginn und Ende der rückwirkenden Überwachung nach Absatz 1 Buchstabe f auf die Regelung in Artikel 4*a* verwiesen (s. die dortigen Erläuterungen).

Art. 74b **Übergangsbestimmung zur Änderung vom 15. November 2023**

Zur Gewährleistung einer einwandfreien Einführung der neuen Auskunfts- und Überwachungstypen bei den FDA und dem Dienst ÜPF ist es vorliegend sinnvoll, detaillierte Übergangsbestimmungen für die einzelnen Änderungen vorzusehen. Innerhalb der vorgesehenen Fristen sind die technischen Anpassungen auf Seiten der FDA und des Dienstes ÜPF sowie die entsprechenden Tests durchzuführen, damit die neuen Auskunfts- und Überwachungstypen so rasch wie möglich, jedoch spätestens bei Ablauf der jeweils vorgesehenen Frist standardisiert durchgeführt werden können. Für AAKD müssen keine Übergangsfristen vorgesehen werden, da die neuen Auskunfts- und Überwachungstypen lediglich für FDA gelten. Die AAKD sind jeweils explizit ausgenommen (s. Erläuterungen zu Art. 18 Abs. 4 und 50 Abs. 1).

Absatz 1 sieht für alle FDA eine Übergangsfrist von 24 Monaten nach Inkrafttreten dieser Verordnungsrevision betreffend die neuen Auskunftstypen gemäss Artikel 48*a* (IR_51_ASSOC_PERM: Auskünfte über längerfristig zugeordnete Identifikatoren) und gemäss Artikel 48*c* (IR_53_TEL_ADJ_NET: Bestimmung der benachbarten Netzte bei Telefonie- und Multimediadiensten) vor. Es ist anzumerken, dass für die FDA mit reduzierten Überwachungspflichten (Art. 51) keine Aufbewahrungspflicht

für die entsprechenden Randdaten gemäss Artikel 48*c* besteht. Sie erteilen daher die Auskünfte gemäss Artikel 48*c* auf der Grundlage der ihnen vorliegenden Informationen. Falls sie die Auskunft ausserhalb des Verarbeitungssystems erteilen, haben sie kaum Aufwand, ihre Systeme anzupassen.

Absatz 2 enthält keine feste Übergangsfrist in Monaten, sondern regelt die Frist für die entsprechende Auskunftsbereitschaft in Abhängigkeit von der tatsächlichen kommerziellen Nutzung der zugrundeliegenden neuen 5G-Funktion des Verbergens des permanenten Teilnehmeridentifikators auf der Funkschnittstelle des mobilen Netzzugangs (sog. 3GPP-Zugang). Betroffen sind die Mobilfunkanbieterinnen, die ein 5G-Netz betreiben. Diese müssen ab Inbetriebnahme ihres ersten kommerziellen Netzzugangs, der die permanenten Identifikatoren auf der Funkschnittstelle verbirgt, was mittels der eigenständigen 5G-Technologie (sog. 5G Standalone) möglich sein wird, den neuen Auskunftstyp gemäss Artikel 48*b* (IR_52_ASSOC_TEMP «sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren») ausführen können, das heisst erst wenn diese neue Funktionalität der 5G-Technologie tatsächlich genutzt wird, muss die automatisierte Abfrage gemäss Artikel 48*b* bei der jeweiligen Anbieterin funktionieren. Dieser Absatz betrifft nur die FDA mit vollen Pflichten. Die FDA mit reduzierten Überwachungspflichten (Art. 51) sind von diesem Auskunftstyp ausgenommen (s. Art. 18 Abs. 4).

Absatz 3 sieht vor, dass für die Umsetzung der beiden neuen Typen der einmaligen, sofortigen Positionsbestimmung nach Artikel 56*a* (RT_56_POS_IMMED) und Artikel 67 Buchstabe b (EP_58_POS_IMMED) wie in Absatz 1 eine Übergangsfrist von 24 Monaten nach Inkrafttreten dieser Verordnungsrevision gewährt wird. Aufgrund des zu erwartenden Zusatznutzens dieser neuen Überwachungstypen sollen sie den Strafverfolgungsbehörden möglichst rasch zur Verfügung stehen. Dieser Absatz betrifft nur die FDA mit vollen Pflichten. Die FDA mit reduzierten Überwachungspflichten (Art. 51) müssen keine Überwachungstypen umsetzen (s. Art. 50 Abs. 1).

Absatz 4 sieht für die Änderung des Auskunftstyps HD_29_TEL betreffend die Bezeichnung des unmittelbar benachbarten Netzes der Kommunikation oder des Kommunikationsversuches (Art. 61 Bst. j) zwei Fristen vor: Erstens müssen die FDA mit vollen Pflichten die Speicherung der hierfür notwendigen Daten innert 18 Monaten nach dem Inkrafttreten dieser Verordnungsrevision sicherstellen. Zweitens müssen sie spätestens 24 Monate nach dem Inkrafttreten dieser Verordnungsrevision diese neuen rückwirkenden Daten liefern können. Die Speicherpflicht beginnt also 6 Monate früher als die Lieferpflicht, damit ab Beginn der Lieferpflicht die entsprechenden historischen Daten der letzten 6 Monate bereits bei den Anbieterinnen zur Verfügung stehen. Dieser Absatz betrifft nur die FDA mit vollen Pflichten. Die FDA mit reduzierten Überwachungspflichten (Art. 51) müssen keine Überwachungstypen umsetzen (s. Art. 50 Abs. 1).

Absatz 5 bestimmt die Übergangsfrist für die FDA mit vollen Pflichten betreffend die beiden neuen Typen der periodischen Positionsbestimmung nach Artikel 56*b* (RT_55_POS_PERIOD) und Artikel 67 Buchstabe c (EP_57_POS_PERIOD). Die Implementierung dieser neuen Überwachungstypen in die aktuelle Echtzeitsystemkomponente des Verarbeitungssystems des Dienstes ÜPF (ISS) ist wirtschaftlich und zeitlich nicht sinnvoll, da diese sich am Ende ihres Lebenszyklus befindet und in ab-

sehbarer Zeit durch eine neue Komponente ersetzt wird. Deshalb wird auf die Implementierung in die aktuelle Komponente (ISS) verzichtet. Zudem ist die Machbarkeit der Implementierung fraglich, da diese Version vom Hersteller nicht mehr weiterentwickelt wird. Deshalb sind diese Überwachungstypen erst nach Einführung und Anpassung der neuen Echtzeitsystemkomponente standardisiert umsetzbar. Die FDA mit vollen Pflichten erhalten nach der Inbetriebnahme der neuen Echtzeitsystemkomponente («FLICC[32] 2.0») noch bis zu 24 Monate Zeit für die nötigen Anpassungsarbeiten in ihren Systemen und für die Durchführung der notwendigen Tests mit dem Dienst ÜPF. Dieser Absatz betrifft nur die FDA mit vollen Pflichten. Die FDA mit reduzierten Überwachungspflichten (Art. 51) müssen keine Überwachungstypen umsetzen (s. Art. 50 Abs. 1).

Absatz 6 bildet das Gegenstück zu den Absätzen 1, 3 und 4 und bestimmt die gleiche Übergangsfrist von 24 Monaten nach dem Inkrafttreten dieser Verordnungsrevision für den Dienst ÜPF betreffend die entsprechenden Auskunfts- und Überwachungstypen (s. Abs. 1, 3 und 4). *Buchstabe a* beinhaltet die Implementierung der neuen Auskunftstypen gemäss den Artikeln 48*a* und 48*c* in die IRC und die Implementierung der beiden neuen Überwachungstypen der einmaligen, sofortigen Positionsbestimmung nach Artikel 56*a* (RT_54_POS_ONCE) und Artikel 67 Buchstabe b (EP_56_POS_ONCE) in die neue Echtzeitsystemkomponente des Verarbeitungssystems des Dienstes ÜPF, damit die Aufträge erteilt sowie die Daten entgegengenommen und für die Benutzer dargestellt werden können. Ausserdem müssen die betreffenden Auskünfte und Überwachungen in der Statistik des Dienstes ÜPF erfasst werden können. *Buchstabe b* regelt analog zu Absatz 4 die Übergangsfrist von 24 Monaten für den Dienst ÜPF, um für die Entgegennahme der entsprechenden historischen Daten (HD) bereit zu sein.

Absatz 7 sieht analog zu Absatz 2 (Art. 48*b*) die gleiche Frist für den Dienst ÜPF vor, um sein Verarbeitungssystem anzupassen, damit die neuen Auskunftsdaten echtzeitnah empfangen und die Auskünfte in der Statistik erfasst werden können.

Absatz 8 bildet das Gegenstück zu Absatz 5 (Art. 56*b* und 67 Bst. c) und legt die gleiche Übergangsfrist für den Dienst ÜPF fest.

Anhang

Bei den Begriffen und Abkürzungen (Anhang VÜPF) werden einige neu in der Verordnung verwendete Begriffe und Abkürzungen hinzugefügt, obsolete entfernt und punktuelle Präzisierungen bei bestehenden Begriffen und Abkürzungen angebracht. Aufgrund der Sortierung in der Reihenfolge der ersten Verwendung des jeweiligen Begriffs oder der jeweiligen Abkürzung in der Verordnung ergeben sich ausserdem Verschiebungen in der Nummerierung.

[32] Federal Lawful Interception Core Component (FLICC)

4.2 Verordnung über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Ersatz von Ausdrücken

Die Abkürzungen (FDA bzw. AAKD) werden auch in der VD-ÜPF benutzt und die entsprechenden Bestimmungen deshalb angepasst.

Art. 1 Geltungsbereich

Da die sichere Kommunikation neu auch für Behörden auf Stufe Departementsverordnung geregelt wird (vgl. Art. 3), ist der Geltungsbereich entsprechend zu erweitern. Deshalb gilt nun die VD-ÜPF samt Anhängen nicht nur für den Dienst ÜPF und die Mitwirkungspflichtigen, sondern auch für die Behörden gemäss Artikel 1 Absatz 2 Buchstaben a-f VÜPF.

Art. 3 Absicherung der Kommunikation

Bisher regelte diese Bestimmung einzig die Kommunikation zwischen den MWP und dem Dienst ÜPF. Die Änderung von Artikel 3 VÜPF, wonach die sicheren Übertragungsmittel durch das EJPD festzulegen sind, führt dazu, dass Artikel 3 VD-ÜPF auch auf die Kommunikation zwischen dem Dienst ÜPF und den Behörden ausgedehnt wird.

Absatz 1 regelt neu auch die sichere Kommunikation zwischen den Behörden (gemäss Artikel 1 Absatz 2 Buchstaben a-f VÜPF) und dem Dienst ÜPF. Die Bestimmung gilt auch für die sichere Kommunikation zwischen dem Dienst ÜPF und den Mitwirkungspflichtigen (gemäss Artikel 2 BÜPF) sowie allenfalls zwischen den Behörden und den Mitwirkungspflichtigen. Als sichere Übertragungsmittel gelten das Verarbeitungssystem des Dienstes ÜPF (*Bst. a*) sowie die Verschlüsselungslösungen für E-Mails (*Bst. b*). Diese sind im Anhang 1 zur VD-ÜPF näher geregelt. Nach Absprache mit dem Dienst ÜPF kann auch ein anderes gleichwertiges Mittel als sicheres Übertragungsmittel gelten (*Bst. c*).

Der frühere Buchstabe a betreffend die vertraulichen Mitteilungen zwischen den MWP und dem Dienst ÜPF wird materiell unverändert in den neuen *Absatz 2* überführt.

Art. 10 Abs. 2bis

Analog der Fristenregelung für die Weiterleitung der Auskunftsgesuche (Art. 14 Abs. 1) beziehungsweise der Aufträge für die Überwachung des Fernmeldeverkehrs (Art. 16 Abs. 1, 17 Abs. 1 und 18 Abs. 1) durch den Dienst ÜPF an die MWP wird in diesem neuen Absatz dieselbe Frist auch für Überwachungen des Postverkehrs geregelt. Die Frist für die Übermittlung des Auftrags zur Ausführung einer Echtzeitüberwachung des Postverkehrs an die Anbieterin von Postdiensten wird ebenfalls auf eine Stunde festgelegt. Die Überwachungen des Postverkehrs werden lediglich während der Normalarbeitszeiten beauftragt und durchgeführt.

Art. 11 Rückwirkende Überwachung

Der neue *Absatz 1* regelt analog zu den Artikeln 10 Absatz 2bis, 14 Absatz 1, 16 Absatz 1, 17 Absatz 1 und 18 Absatz 1 die Frist für die Übermittlung des Auftrags zur Durchführung einer rückwirkenden Überwachung des Postverkehrs (s. Erläuterungen zu Art. 10 Abs. 2bis).

Absatz 2 entspricht dem bisherigen Artikel 11.

Art. 14 Abs 2, 3 und 4

In *Absatz 2* werden die Bearbeitungszeiten für folgende MWP gemeinsam geregelt: die FDA, ohne die FDA mit reduzierten Überwachungspflichten (Art. 51 VÜPF), die AAKD mit weitergehenden Auskunftspflichten (Art. 22 VÜPF) und die AAKD mit weitergehenden Überwachungspflichten (Art. 52 VÜPF). Es wird die Einschränkung angefügt, dass die nachfolgenden Regelungen nur insofern gelten, wie die MWP nach Artikel 18 VÜPF zur entsprechenden Auskunftserteilung verpflichtet sind. Die AAKD mit weitergehenden Pflichten gemäss Artikel 22 oder 52 VÜPF sind gemäss Artikel 18 Absatz 4 VÜPF von den drei neuen Auskunftstypen gemäss Artikel 48*a*–48*c* VÜPF befreit.

In *Buchstabe a* wird präzisiert, dass der Auskunftstyp nach Artikel 48*b* VÜPF sofort zu beantworten ist. Die Antwortzeit dieses neuen Auskunftstyps muss sehr kurz sein (im Bereich von Sekundenbruchteilen), da sich die temporären Identifikatoren oft ändern. Diese Auskunft muss daher automatisiert über eine neue Abfrageschnittstelle abgefragt und erteilt werden. Ein massgeblicher Zeitpunkt kann nicht angegeben werden, da es eine Echtzeitabfrage ist. Es gilt der Zeitpunkt der Abfrage. Abfragen in die Vergangenheit sind nicht möglich. Anzumerken ist, dass die FDA mit reduzierten Überwachungspflichten, was auch aus dem Einleitungssatz hervorgeht, sowie die AAKD mit weitergehenden Pflichten gemäss Artikel 22 oder 52 VÜPF aus Gründen der Verhältnismässigkeit von der Auskunftserteilung nach Artikel 48*b* VÜPF befreit sind (s. Art. 18 Abs. 3 und 4 VÜPF). Auf sie ist Buchstabe a nicht anwendbar ist.

In *Buchstabe b* bleibt die Frist von einer Stunde für die Bearbeitung der genannten Auskünfte durch die Anbieterin unverändert. Da die aufgeführten Auskunftstypen automatisiert beantwortet werden (s. Art. 18 Abs. 2 VÜPF), sind die Reaktionszeiten zu deren Beantwortung entsprechend kurz angesetzt. Es handelt sich um folgende Auskunftstypen: IR_4_NA (Art. 35), IR_5_NA_FLEX (Art. 27 i. V. m. Art. 35), IR_6_NA (Art. 36), IR_7_IP (Art. 37), IR_10_TEL (Art. 40), IR_11_TEL_FLEX (Art. 27 i. V. m. Art. 40), IR_12_TEL (Art. 41). Die einstündige Frist gilt auch für den neuen Auskunftstyp gemäss Artikel 48*a* (IR_51_ASSOC_PERM: Auskünfte über längerfristig zugeordnete Identifikatoren). Es ist zu beachten, dass bei automatisierten Auskunftsgesuchen die Avisierung des Dienstes ÜPF im Pikett entfällt.

In *Buchstabe c Ziffer 1* bleibt die Beantwortungsfrist von einem Arbeitstag für Auskunftsgesuche, die während den Normalarbeitszeiten bei der Anbieterin eingehen, bestehen. Von dieser Frist betroffen sind wie bisher die folgenden «manuellen» Auskunftstypen: IR_8_IP (NAT) (Art. 38), IR_9_NAT (Art. 39), IR_15_COM (Art. 43), IR_16_COM_FLEX (Art. 27 i. V. m. Art. 43). Neu wird die Bearbeitungsfrist für die Auskunftstypen IR_13_EMAIL (Art. 42) und IR_14_EMAIL_FLEX (Art. 27 i. V. mit Art. 42) einen Arbeitstag beziehungsweise sechs Stunden anstatt eine Stunde

sein (s. bisherige Abs. 2 Bst. a), da dieser Auskunftstyp neu auch manuell erteilt werden kann (s. Erläuterungen zu Art. 18 Abs. 2 VÜPF). Hinzugekommen ist auch der neu eingeführte Auskunftstyp IR_53_TEL_ADJ_NET (Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten; Art. 48*c* VÜPF). «Innerhalb eines Arbeitstages» bedeutet, dass die Antwort spätestens bis um 17.00 Uhr des darauffolgenden Arbeitstages beim Dienst ÜPF beziehungsweise der anfragenden Behörde eintreffen muss (s. Bsp. 1 hier unten).

In der Praxis wurde diese Frist von einem Arbeitstag von den auskunftsberechtigten Behörden als zu lang erachtet, wenn ihre Anfragen an Wochenenden oder Feiertagen gestellt wurden und daher dringend waren. Aus diesem Grund wird in *Ziffer 2* für diese Auskunftsgesuche ausserhalb der Normalarbeitszeiten und an Feiertagen neu eine kürzere Frist von sechs Stunden festgesetzt. Diese Frist entspricht derjenigen für dringende rückwirkende Überwachungen. Im Pikett gibt es erfahrungsgemäss nur wenige Auskunftsgesuche und Überwachungsanordnungen, dafür sind diese dringend und können nicht bis zum nächsten Arbeitstag warten. Daher ist nicht mit einer Überlastung der MWP zu rechnen. Andererseits müssen die Strafverfolgungsbehörden auch an Wochenenden und Feiertagen dringend benötigte Auskünfte einholen können, damit die polizeilichen Ermittlungen und somit die Strafverfolgung nicht behindert werden. Anzumerken ist, dass Ziffer 2 nur für MWP gilt, die gemäss Artikel 11 Absatz 1 VÜPF einen Pikettdienst zur Verfügung stellen müssen, was für die FDA mit reduzierten Überwachungspflichten (Art. 51 VÜPF) sowie die AAKD mit weitergehenden Auskunftspflichten (Art. 22 VÜPF) nicht der Fall ist. Auf sie ist Buchstabe c Ziffer 2 nicht anwendbar.

Ein nicht automatisiertes Auskunftsgesuch im Pikett an die betroffene MWP setzt voraus, dass der Dienst ÜPF durch die auskunftsberechtigte Behörde (s. Art. 15 BÜPF) avisiert wird (vgl. Art. 11 Abs. 2 VÜPF), damit er anschliessend die betroffene MWP für den entsprechenden Auftrag kontaktieren kann.

Die Bearbeitungszeit von sechs Stunden bedeutet, dass die MWP die Antwort innerhalb von sechs Stunden ab Eintreffen des Gesuchs bei der MWP in die Komponente IRC (vgl. Erläuterungen zu Art. 18 VÜPF) einzugeben oder, im Falle einer Störung der IRC, gesichert (s. Art. 3) an den Dienst ÜPF zu senden hat. Anbei einige Beispiele betreffend Auskunftsgesuche nach Buchstabe c:

Beispiel 1: Ein Auskunftsgesuch wird am Montag um 16.10 Uhr in die IRC eingegeben und trifft innert weniger Sekunden bei der MWP ein. In diesem Fall beträgt die Frist einen Arbeitstag. Die Anbieterin hat bis zum Ende des nächsten Arbeitstages Zeit, d. h. bis am Dienstag um 16.59 Uhr, um das Auskunftsgesuch zu beantworten.

Beispiel 2: Ein Auskunftsgesuch wird am Montag um 17.05 Uhr in die IRC eingegeben und trifft innert weniger Sekunden bei der MWP ein. Da dieser Zeitpunkt ausserhalb der Normalarbeitszeiten liegt, muss die auskunftsberechtigte Behörde den Dienst ÜPF avisieren, wenn sie möchte, dass das Gesuch im Pikett behandelt wird. Der Dienst ÜPF informiert unverzüglich die MWP. Die Bearbeitungsfrist, die der MWP gewährt wird, beträgt sechs Stunden ab Auftragseingang. Die Anbieterin hat bis am selben Tag um 23.05 Uhr Zeit, um das Auskunftsgesuch zu beantworten.

Beispiel 3: Wenn das Auskunftsgesuch am Samstag um 18.50 Uhr (ausserhalb der Normalarbeitszeiten) gestellt wird, hat die Anbieterin bis am Sonntag um 00.50 Uhr Zeit für die Bearbeitung des Gesuchs. Der Ablauf ist analog wie in Beispiel 2.

Auch für manuelle Auskünfte gemäss Buchstabe d beträgt die Beantwortungsfrist einen Arbeitstag. Da die Auskünfte gemäss den Artikeln 44–48 während dem Pikettdienst nicht zwingend erbracht werden müssen, werden diese nicht im vorangehenden Buchstaben c, sondern separat geregelt. Für die Auskünfte IR_17_PAY (Art. 44), IR_18_ID (Art. 45), IR_19_BILL (Art. 46), IR_20_CONTRACT (Art. 47) und IR_21_TECH (Art. 48) bleibt die Beantwortungsfrist im Vergleich zum bisherigen Artikel 14 Absatz 2 Buchstabe b unverändert.

In *Absatz 3* werden die Bearbeitungszeiten für die «kleinen» MWP geregelt. Hierunter fallen die FDA mit reduzierten Überwachungspflichten (Art. 51).

Analog zu Absatz 2 Buchstabe a und b wird betreffend die Bearbeitungsfristen ein Unterschied hinsichtlich der Komplexität der Auskunftserteilung gemacht. Für die in *Buchstabe a* aufgeführten Auskünfte wird die Frist im Vergleich zum bisherigen Recht von zwei auf einen Arbeitstag reduziert. Bei den in Buchstabe b genannten Auskünften bleibt die Frist unverändert (zwei Arbeitstage).

In *Absatz 4* werden die Bearbeitungszeiten für AAKD ohne weitergehende Pflichten gemäss Artikel 22 oder 52 VÜPF und für die Betreiberinnen interner Fernmeldenetze geregelt, welche lediglich die ihnen vorliegenden Angaben zu liefern haben (vgl. Art. 22 Abs. 3 BÜPF). Diese Mitwirkungspflichtigen müssen sich bei der Auskunftserteilung nicht an die standardisierten Typen der VÜPF halten (Art 18*a* VÜPF).

Zu den Bearbeitungszeiten siehe auch die Tabelle in Anhang «Übersicht Bearbeitungszeiten».

Art. 18 Abs. 2 und 3

Infolge der neuen Buchstaben in Artikel 67 und 68 Absatz 1 VÜPF müssen die Verweise in *Absatz 2* und *Absatz 3* ebenfalls angepasst werden.

Anhang 1

Im Rahmen der Teilrevision der VÜPF werden drei neue Auskunfts- und vier neue Überwachungstypen geschaffen:

1) der Auskunftstyp IR_51_ASSOC_PERM, Auskünfte über längerfristig zugeordnete Identifikatoren (Art. 48*a* VÜPF);
2) der Auskunftstyp IR_52_ASSOC_TEMP, sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren (Art. 48*b* VÜPF);
3) der Auskunftstyp IR_53_TEL_ADJ_NET, Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten (Art. 48*c* VÜPF);
4) der Überwachungstyp (Echtzeitüberwachung) RT_54_POS_ONCE, einmalige, sofortige Positionsbestimmung durch das Netzwerk (Art. 56*a* VÜPF);
5) der Überwachungstyp (Echtzeitüberwachung) RT_55_POS_PERIOD, periodisch wiederkehrende Positionsbestimmung durch das Netzwerk (Art. 56*b* VÜPF);

6) der Überwachungstyp (Notsuche) EP_56_POS_ONCE, einmalige, sofortige Positionsbestimmung durch das Netzwerk (Art. 67 Bst. b VÜPF); sowie
7) der Überwachungstyp (Notsuche) EP_57_POS_PERIOD, periodisch wiederkehrende Positionsbestimmung durch das Netzwerk (Art. 67 Bst. c VÜPF).

Dies erfordert eine Teilrevision des Anhangs 1 der VD-ÜPF, um die entsprechenden Vorschriften für die Schnittstellen zur Durchführung der Fernmeldeüberwachung festzulegen. Ausserdem werden Parameter und Bezeichnungen der 5G-Technologie eingefügt.

Anhang 2

Anhang 2 der VD-ÜPF definiert die technischen Anforderungen an die Ausleitungsnetze für die Fernmeldeüberwachung zwischen den MWP und dem Verarbeitungssystem des Dienstes ÜPF. Hauptauslöser für die Teilrevision dieses Anhangs war der Wegfall der ISDN-Technologie bei schweizerischen FDA im Zuge des technischen Fortschritts und damit die Ausserbetriebsetzung der existierenden ISDN-Ausleitungsverbindungen. ISDN beruhte noch auf dem Prinzip der Leitungsvermittlung. Inzwischen werden als Ausleitungsnetz nur noch paketvermittelte Netze unterstützt. Die ISDN betreffenden Abschnitte des Anhangs 2 wurden komplett gestrichen. Es entfallen die ISDN-Übergabeschnittstellen (HI2 für CS IRI und HI3 für CS CC), das ISDN-Ausleitungsnetz für CS CC, das Ausleitungsnetz für CS IRI und die Signalisierungssequenzen für das leitungsvermittelte (CS) Ausleitungsnetz. Falls eine MWP noch Überwachungsdaten aus leitungsvermittelten Netzen übermitteln möchte, müssen diese in IP-Pakete konvertiert und über paketvermittelte Netze ausgeleitet werden.

Ausserdem werden die Übersicht über die Übergabeschnittstellen, die Ausführungen über die einzelnen Instanzen und Komponenten des Verarbeitungssystems und das Schweizer Referenzmodell für die Fernmeldeüberwachung (funktionale Architektur für die Fernmeldeüberwachung, basierend auf der ETSI Referenzarchitektur) aktualisiert.

Des Weiteren werden einige Begriffe bereinigt und die Schnittstelle LI_HIQR (für Auskünfte gemäss Art. 48*b*) sowie eine Referenz auf die VVS-ÜPF hinzugefügt.

4.3 Verordnung über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (VVS-ÜPF)

Art. 3 Abs. 2 Bst. a-c

In *Absatz 2* werden die *Buchstaben a-c* mit dem Verweis auf den 1. Abschnitt des 3. Kapitels der VÜPF ergänzt, so dass klar hervorgeht, dass auch für die darin enthaltenen Artikel, wie Artikel 25 (Besondere Auskünfte und Überwachungen) und 27 (Auskunftstypen mit flexibler Namenssuche) VÜPF, die Bearbeitung der Daten im Verarbeitungssystem zur Fernmeldeüberwachung (V-FMÜ) möglich ist. Mit der

neuen Echtzeitüberwachungskomponente sollen immer mehr Daten aus besonderen Überwachungen («special cases») ebenfalls mit dem V-FMÜ an die Strafverfolgungsbehörden ausgeliefert werden. Der bisherige Inhalt der Bestimmung bleibt weiterhin gültig. Absatz 2 Buchstabe d bleibt unverändert.

Art. 8 Abs. 3-6

Nach *Absatz 3* können einzelne Mitarbeitende (sog. «OrgAdmin»), vor allem der Polizei, durch den Dienst ÜPF berechtigt werden, Zugriffe weiter zu vergeben. Sie können weiterhin die Zugriffe nur «innerhalb ihrer Behörde» oder an betroffene Personen und deren Rechtsbeistände vergeben. Die Zugriffe sollen neu auch an die jeweils zuständige genehmigende Behörde vergeben werden können. Darunter sind die Zwangsmassnahmengerichte beziehungsweise für den NDB das Bundesverwaltungsgericht zu verstehen. Die im Anhang unter Ziffer 2.7 «Genehmigende Behörde» vorgesehenen Berechtigungen ändern sich nicht. Diese Berechtigungen konnten bisher lediglich durch den Dienst ÜPF vergeben werden. Neu soll dies nun auch durch die OrgAdmin möglich sein. Die genehmigende Behörde erhält dabei lediglich einen Zugriff auf die Auftragsmanagementkomponente WMC (Warrant Management Component) und hat somit keinen Zugriff auf Daten aus der Post- und Fernmeldeüberwachung an sich.

Im Rahmen der Vernehmlassung wurde der Wunsch geäussert, dass die vom Dienst ÜPF berechtigten Mitarbeitenden (OrgAdmin) der auswertenden, anordnenden und genehmigenden Behörden ihrerseits berechtigt würden, Berechtigungen auch ausserhalb ihrer eigenen Behörde zu vergeben. Dies würde die Zusammenarbeit vereinfachen und den Dienst ÜPF von dieser administrativen Aufgabe entlasten, insbesondere im Dringlichkeitsfall (z. B. bei Notsuchen, die oftmals ausserhalb der Bürozeiten durchgeführt werden müssen). Dieser Änderungsantrag konnte nicht nachgekommen werden, da Artikel 9 Absatz 1 BÜPF verletzt würde, wonach der Dienst ÜPF selber die Zugriffe auf die im betreffenden Verfahren gesammelten Daten zu gewähren hat.

Neu wird in den Absätzen 4 und 5 der Zugriff auf die Daten durch den Dienst ÜPF ausgeführt. Die Mitarbeitenden des Dienstes ÜPF sowie mögliche weitere Hilfspersonen haben grundsätzlich keinen Zugang auf Daten aus einzelnen Überwachungen. Die Daten werden meist lediglich durch eine Software gescannt. Eine Kenntnisnahme vom Inhalt der Daten durch eine Person ist in der Regel nicht vorgesehen («privacy by design»). Trotzdem wird sowohl bei den Mitarbeitenden des Dienstes ÜPF wie auch bei weiteren Personen, welche den Dienst ÜPF in seinem Auftrag unterstützen, in der Regel eine Personensicherheitskontrolle durchgeführt. Hilfe von weiteren Personen kann notwendig werden, wenn beispielsweise Spezialisten der Betreiberin der Hardware oder der Lieferantin von Software komplexe Probleme lösen helfen. Hilfspersonen können aber auch Personen sein, welche den Dienst ÜPF bei hohem Arbeitsanfall unterstützen. Der Dienst ÜPF hat nach den Artikeln 18 Absatz 1 BÜPF und 29 VÜPF die Aufgabe, Massnahmen zur Qualitätskontrolle der von den Anbieterinnen gelieferten Überwachungsdaten zu ergreifen.

Absatz 4 führt den in Artikel 18 Absatz 2 BÜPF festgehaltenen Grundsatz aus, wonach der Dienst ÜPF bei der Qualitätskontrolle mit vorgängiger Zustimmung der mit

dem Verfahren befassten Behörde vom Inhalt der Daten Kenntnis nehmen darf. Hierbei kann es sich um Probleme handeln, die die anordnenden Behörden selbst feststellen, wie ein Telefonat, bei dem nur ein Teilnehmer statt beiden zu hören ist.

Nicht nur zur Qualitätskontrolle, sondern auch zur Beratung der anordnenden oder anderweitig berechtigten Behörde (Art. 16 Bst. j BÜPF) sowie zur Sicherstellung des ordnungsgemässen Funktionierens des Verarbeitungssystems des Dienstes ÜPF (V-FMÜ) können Zugriffe auf Überwachungsdaten und somit die Kenntnisnahme von einzelnen Inhaltsdaten notwendig werden. Der Dienst ÜPF hat in diesen Fällen immer, wenn möglich im Voraus, die schriftliche Zustimmung der mit dem Verfahren befassten Behörde einzuholen. Die Schriftlichkeit nach Absatz 4 ist erforderlich, weil die Einwilligung nachweisbar sein muss. In ähnlicher Weise schreibt auch Artikel 11 Absatz 1 Buchstabe b VDTI[33] die schriftliche Zustimmung der zuständigen Behörde vor. Die Anforderungen an die Schriftlichkeit nach Artikel 14 OR[34] müssen dabei nicht eingehalten werden. Die Einwilligung muss also nicht mit einer Unterschrift oder einer qualifizierten elektronischen Signatur versehen sein. Dem Erfordernis der Schriftlichkeit genügt auch ein einfaches E-Mail.

Der Dienst ÜPF hat nach Artikel 6 BÜPF die Aufgabe, ein Informatiksystem zur Bearbeitung der Daten aus der Überwachung des Fernmeldeverkehrs, das V-FMÜ, zu betreiben. Um dieses sicher ausführen zu können, sind in Absatz 5 Ausnahmen zu Absatz 4 vorgesehen. Der Dienst ÜPF ist für die Sicherheit des V-FMÜ verantwortlich und hat somit entsprechende Massnahmen zu treffen (Art. 12 BÜPF, Art. 11 VVS-ÜPF), bei welchen nicht immer eine Zustimmung der mit dem Verfahren befassten Behörde eingeholt werden soll (vgl. Abs. 5). Dabei ist sowohl an präventive Massnahmen, wie Funktionstests, statistisch gestützte Beobachtung der Aktivitäten im System, wie auch an reaktive Eingriffe bei bereits festgestellten Funktionsstörungen zu denken. Zu diesem Zweck führt der Dienst ÜPF ein Monitoring zur Qualitätskontrolle durch. Es wird geprüft, ob das System richtig funktioniert und ob plausibel ist, was dargestellt wird (Lesbarkeit, Inhalt nutzbar, verwertbar). Die Mitarbeitenden des Dienstes ÜPF sowie allfällige Hilfspersonen (z. B. Spezialisten einer Anbieterin von eingesetzter Software) benötigen den Zugang auf verschiedene Daten (wie Rand-, Log-, Inhaltsdaten) der Überwachung. Dabei kann es vorkommen, dass sie auch vom Inhalt der Überwachung Kenntnis nehmen müssen, auch wenn dies nicht ihr primäres Ziel oder ihre Absicht ist. In anderen Worten ist der Mitarbeitende des Dienstes ÜPF auf das Problem fokussiert, das zu lösen ist, und nimmt meist nur Bruchstücke des Inhalts der Daten wahr. In der Regel werden automatisierte Zugriffe vorgenommen, um die Datenqualität und die Systemstabilität regelmässig zu überprüfen sowie allfällige Fehler frühzeitig beheben zu können. Dabei werden unter anderem die Ausbreitung der Fehler (Betrifft es nur einen Einzelfall?), die Tragweite (Ist die Datenlieferung verspätet, fehlerhaft oder nicht vorhanden?) sowie die Dauer und die Faktoren, welche das Fehlerbild kennzeichnen (Welche Überwachungstypen, welche Provider sind betroffen?), untersucht.

33 Verodnung vom 25.11.2020 über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (Verordnung über die digitale Transformation und die Informatik; **VDTI**; SR **172.010.58**)

34 Bundesgesetz vom 30.03.1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil : Obligationenrecht ; **OR** ; SR **220**)

Absatz 5 hält die Ausnahmen zu Absatz 4 fest, in welchen von einer Zustimmung der mit dem Verfahren befassten Behörde abgesehen werden darf.

Zur Sicherstellung des ordnungsgemässen Funktionierens, wie bei drohenden oder eingetretenen gravierenden Funktionsstörungen (*Bst. a Ziff. 1),* wird ein Zugriff rasch benötigt, um die Ursachen zu finden, damit die Funktionsstörung behoben werden kann (vgl. auch Art. 11). Auch eine drohende Gefährdung für das System genügt, da auch diese einen Notfall darstellt, wo sofort gehandelt werden muss. Wenn beispielsweise eine Überwachung einer Behörde sehr schnell riesige Mengen an Speicherplatz benötigt und die entsprechende Behörde nicht erreicht werden kann, weil sie nur zu Bürozeiten erreichbar ist, muss auch bereits bei einer drohenden Gefährdung des V-FMÜ auf die Daten zugegriffen werden können, um das Problem zu finden und so das stabile Laufen des V-FMÜ zu gewährleisten.

Auch in Fällen (*Bst. a Ziff. 2*), wo es unmöglich ist, vorgängig herauszufinden, welche Überwachung ein Problem verursacht oder dies einen unverhältnismässig hohen Aufwand verursachen würde, soll der Dienst ÜPF die Möglichkeit haben, entsprechende Massnahmen zur Sicherstellung des ordnungsgemässen Funktionierens des V-FMÜ ergreifen zu können. So auch, wenn die zuständige Behörde in der zur Verfügung stehenden Zeit nicht erreicht werden kann (z. B. an Feiertagen) oder sie zu kontaktieren, einen unverhältnismässigen Aufwand generieren würde. Bereits eine kleine Änderung in der Übermittlung von Produkten oder Formaten durch die MWP kann im V-FMÜ zu einer falschen oder andersartigen Darstellung führen, was wiederum Schwierigkeiten bei der Auswertung der Daten durch die zuständigen Behörden hervorrufen könnte. Bei der Einspeisung respektive Umwandlung der von den MWP in guter Qualität gelieferten Daten kann es ebenfalls zu Qualitätsverlusten oder gar zu Problemen des ganzen V-FMÜ kommen. Unter Umständen ist dies nur mit ausführlicheren Analysen der Daten feststellbar und kann somit im Voraus nicht einer konkreten Überwachung beziehungsweise einer bestimmten Behörde zugeordnet werden, so dass keine bestimmte Zustimmung eingeholt werden kann.
Nach *Buchstabe b* ist die Zustimmung ebenfalls nicht erforderlich, wenn es aufgrund der grossen Anzahl der vom Zugriff betroffenen Überwachungen unverhältnismässig ist, alle zuständigen Behörden zu kontaktieren. In diesen Fällen funktioniert das System zwar noch ordnungsgemäss, könnte allerdings instabiler laufen oder an Qualität verlieren. Gerade zur Feststellung, welche Überwachungen oder welche Formate ein Problem verursachen oder um das System generell stabiler laufen zu lassen (wie beim erwähnten Monitoring), sind oft sehr viele Daten zur Feststellung von Anomalien zu vergleichen, dies meist maschinell. Für die maschinelle Analyse der Daten muss meist auf eine grosse Anzahl von Überwachungen aus verschiedenen Anordnungen und von verschiedenen Behörden zugegriffen werden, bis die Problematik gefunden werden kann. Dabei ist es im Voraus schwierig abzuschätzen, wie viele und welche Überwachungen von einer Problematik betroffen sind. In einem solchen Fall alle zuständigen Behörden zu eruieren und diese einzeln zu kontaktieren, ist nahezu unmöglich oder mit einem unverhältnismässig hohen Aufwand verbunden. Wenn eine Problematik demnach nur dank dem Zugriff auf eine grosse Anzahl von Überwachungen gelöst werden kann, ist deshalb die Zustimmung aller einzelner Behörden nicht erforderlich.

Absatz 6 sieht vor, dass der Dienst ÜPF angemessene vertragliche, organisatorische und technische Vorkehrungen ergreift, um eine weitere Verbreitung der Daten zu verhindern. Dadurch soll sichergestellt werden, dass alle Personen, also nicht nur Dritte (z. B. Hilfspersonen vom Dienst ÜPF), sondern auch die Mitarbeitenden des Dienstes ÜPF, welche zur Erfüllung ihrer Aufgaben Kenntnis von den Überwachungsdaten nehmen müssen, diese nicht an weitere Personen bekannt geben.

Artikel 6 DSV[35] stellt eine ausreichende Rechtsgrundlage dar, wonach der Dienst ÜPF die Absätze 3-6 im Bearbeitungsreglement zu präzisieren hat. Der Inhalt des bisherigen Absatzes 4 braucht deshalb nicht in den neuen Artikel 8 übernommen zu werden.

Art. 10 Abs. 4

Die Aufbewahrungsfristen für Daten im V-FMÜ sind in Artikel 11 BÜPF aufgeführt.

Absatz 4 regelt die Aufbewahrungsdauer der Protokolle. Hier wird das Wort Speicherdauer durch den treffenderen Ausdruck Aufbewahrungsdauer ersetzt.

Auch die Vernichtung von Daten ist zu protokollieren. Allerdings fehlte bislang eine Regelung, wie lange die Protokolle der Vernichtung der Daten aufzubewahren sind. Dies wird mit dem neuen *zweiten Satz* geregelt. So soll vor allem nachvollzogen werden können, wann welche Daten gelöscht wurden, die vorher mit verminderten Bearbeitungsfunktionen über einen längeren Zeitraum aufbewahrt wurden. Artikel 4 DSV kann hier nicht herangezogen werden.

Art. 11 Massnahmen für die Systemsicherheit

Im *ersten Satz* wird der etwas unpräzise und enge Begriff des «ordentlichen Betriebs» durch den ebenfalls in Artikel 8 Absatz 4 genannten Begriff «ordnungsgemässen Funktionierens» ersetzt. Der *zweite* Satz übernimmt grundsätzlich die bisherige Regelung, wonach der Dienst ÜPF die durch die Störung betroffene Behörde anhört, soweit es möglich ist, sie zu kontaktieren (s. Art. 8 Abs. 5).

Anhang Bst. af

Die «Anzeige Betriebslage der Teile des Verarbeitungssystems, auf welche die Person Zugriff hat», das sogenannte PTSS-Dashboard, ist eine Anwendung, welche dazu dient, den Zustand der Überwachungskomponenten zu visualisieren. PTSS ist die englische Bezeichnung für den Dienst ÜPF. Auf dieser Anwendung werden Tickets und Meldungen (z. B. Störungsmeldungen und deren Status, Zustandsanzeigen der Systemkomponenten, Stabilität der Netzwerke), sowie Fristen (z. B. Wartungsfenster für Systemkomponenten, andere Systeme wie I-Net von Teldas) veröffentlicht. Unter anderem verarbeitet das PTSS-Dashboard auch Daten aus dem aktuellen Betriebszustand der Echtzeitüberwachungskomponente und kann diese grafisch darstellen. Mit dieser Ergänzung der Matrix wird der Zugriff der berechtigten Behörden und des Dienstes ÜPF auf das PTSS-Dashboard geregelt, wobei der Zugriff auf das PTTS-

[35] Verordnung vom 31.08.2022 über den Datenschutz (**Datenschutzverordnung**; **DSV** ; SR **235.11**)

Dashboard und der Umfang der angezeigten Daten grundsätzlich von den effektiven Zugriffsrechten der jeweiligen Person auf die Komponenten des V-FMÜ abhängt.

5 Auswirkungen

5.1 Auswirkungen auf den Bund

Die vorgesehenen Anpassungen der drei Ausführungsverordnungen des BÜPF (VÜPF, VD-ÜPF und VVS-ÜPF) werden aus heutiger Sicht keine erheblichen finanziellen und personellen Auswirkungen für den Bund haben.

Die Integrierung der neuen Auskunfts- und Überwachungstypen in den entsprechenden Komponenten des Verarbeitungssystems des Dienstes ÜPF wird gewisse Anpassungen im System (zusätzliche Prozessabläufe, Änderungen der Funktionalitäten, allfällige neue Server usw.) mit sich ziehen. Für den Dienst ÜPF rechnet man deshalb mit zusätzlichen Ausgaben, die aber mit den aktuell budgetierten Mitteln umgesetzt werden können.

5.2 Auswirkungen auf Kantone

Auch für die Kantone werden die vorgesehenen Anpassungen aus heutiger Sicht keine erheblichen finanziellen und personellen Auswirkungen haben. Die Gebühren für die neuen Auskunfts- und Überwachungstypen werden mit den Pauschalen der FV-VÜPF (separate Vorlage) berücksichtigt.

5.3 Auswirkungen auf die MWP

Die neuen Auskunfts- und Überwachungstypen und die Anpassungen an die 5G-Technologie in der VÜPF können für die FDA finanzielle und wirtschaftliche Konsequenzen haben, je nachdem, welche technischen Anpassungen sie an ihren Systemen infolge dieser Teilrevisionen vornehmen müssen. Insbesondere für die Implementierung der neuen Auskunfts- und Überwachungstypen werden die FDA Investitionskosten haben. Gemäss Artikel 74*b* VÜPF erhalten FDA längere Fristen (24 Monate anstelle von 12), um ihre Systeme an die neuen Auskunfts- und Überwachungstypen anzupassen.

6 Rechtliche Aspekte

6.1 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die Vorlage ist mit internationalen Verpflichtungen der Schweiz vereinbar.

6.2 Erlassform

Es handelt sich hier um eine Teilrevision einer Verordnung des Bundesrates im Sinne von Artikel 182 BV[36].

6.3 Subdelegation von Rechtsetzungsbefugnissen

Die Vorlage enthält keine Subdelegation von Rechtsetzungsbefugnissen (s. aber Art. 70 VÜPF und die VD-ÜPF).

6.4 Datenschutz

Die vorgesehenen Änderungen betreffen auch die Bearbeitung besonders schützenswerter Personendaten (Art. 4 BÜPF).

Anhang

Tabelle «Übersicht Bearbeitungszeiten»

36 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999 (**BV**; SR **101**)

Tabelle «Übersicht Bearbeitungszeiten»

Auftrag	**VÜPF Art.**	**Auftragstypen**	**Dienst ÜPF**	**Postanbieterinnen**
Echtzeitüberwachung Post während der Bürozeiten	16 Bst. a 16 Bst. b	PO_1_RT_INTERCEPTION PO_2_RT_DELIVERY	≤ 1 Stunde	≤ 1 Arbeitstag
Rückwirkende Überwachung Post während der Bürozeiten	16 Bst. c	PO_3_HD	≤ 1 Stunde	≤ 3 Arbeitstage
Deaktivierungen nur während der Bürozeiten	16 Bst. a	PO_1_RT_INTERCEPTION	≤ 1 Stunde	≤ 1 Arbeitstag

Auftrag	VÜPF Art.	Auftragstypen	Dienst ÜPF	FDA mit vollen Pflichten* AAKD mit weitergehenden Auskunftspflichten (Art. 22 VÜPF) AAKD mit weitergehenden Überwachungspflichten (Art. 52 VÜPF)	FDA mit reduzierten Überwachungspflichten (Art. 51 VÜPF)
Auskünfte	35 27, 35 36 37 40 27, 40 41 48*a*	IR_4_NA IR_5_NA_FLEX IR_6_NA IR_7_IP IR_10_TEL IR_11_TEL_FLEX IR_12_TEL IR_51_ASSOC_PERM**	≤ 1 Stunde	≤ 1 Stunde	≤ 1 Arbeitstag
	48*b*	IR_52_ASSOC_TEMP**	sofort	Sofort (ausgenommen AAKD mit weitergehenden Auskunftspflichten, Art. 22 VÜPF)	--
	38 39 42 27, 42 43 27, 43 48*c*	IR_8_IP (NAT) IR_9_NAT IR_13_EMAIL IR_14_EMAIL_FLEX IR_15_COM IR_16_COM_FLEX IR_53_TEL_ADJ_NET**	≤ 1 Stunde	Eingang während der Normalarbeitszeiten: ≤ 1 Arbeitstag Eingang ausserhalb der Normalarbeitszeiten und an Feiertagen: ≤ 6 Stunden (ausgenommen AAKD mit weitergehenden Auskunftspflichten, Art. 22 VÜPF)	≤ 2 Arbeitstage
	44 45 46 47 48	IR_17_PAY IR_18_ID IR_19_BILL IR_20_CONTRACT IR_21_TECH	≤ 1 Stunde	≤ 1 Arbeitstag	≤ 2 Arbeitstage

Auftrag	**VÜPF Art.**	**Auftragstypen**	**Dienst ÜPF**	**FDA mit vollen Pflichten*** **AAKD mit weitergehenden Überwachungspflichten (Art. 52 VÜPF)**
Echtzeitüberwachung während der Bürozeiten	54 55 56 56*a* 56*b* 57 58 59 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 1 Stunde	≤ 1 Stunde
Echtzeitüberwachung per Datum während der Bürozeiten	54 55 56 56*a* 56*b* 57 58 59 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 1 Stunde	Zu dem im Auftrag angegebenen Zeitpunkt einzurichten (> 1 Stunde)
Echtzeitüberwachung während des Piketts	54 55 56 56*a* 56*b* 57 58 59 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 1 Stunde	≤ 2 Stunden
Rückwirkende Überwachung während der Bürozeiten	60 61 62 63 64 65	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV**** AS_33_PREP_REF	≤ 1 Stunde	≤ 3 Arbeitstage

	66	AS_34		
Rückwirkende Überwachung in dringenden Fällen (während der Bürozeiten und des Piketts)	60 61 62 63 64 65 66	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV**** AS_33_PREP_REF AS_34	≤ 1 Stunde	≤ 6 Stunden
Notsuchen während der Bürozeiten und des Piketts	67 Bst. a 67 Bst. b 67 Bst. c 67 Bst. d 67 Bst. e	EP_35_PAGING EP_56_POS_ONCE*** EP_57_POS_PERIOD*** EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 Stunde	≤ 1 Stunde
	67 Bst. f	EP_38_HD	≤ 1 Stunde	≤ 4 Stunden
Fahndungen während der Bürozeiten und des Piketts	68 Abs. 1 Bst. a 68 Abs. 1 Bst. e 68 Abs. 1 Bst. d 68 Abs. 1 Bst. e 68 Abs. 1 Bst. d 68 Abs. 1 Bst. e 68 Abs. 1 Bst. d 68 Abs. 1 Bst. b 68 Abs. 1 Bst. c	HD_31_PAGING RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD***	≤ 1 Stunde	≤ 1 Stunde
Fahndungen während der Bürozeiten und des Piketts	68 Abs. 1 Bst. f 68 Abs. 1 Bst. f 68 Abs. 1 Bst. f 68 Abs. 1 Bst. g 68 Abs. 1 Bst. g 68 Abs. 1 Bst. g	HD_28_NA HD_29_TEL HD_30_EMAIL AS_32_PREP_COV**** AS_33_PREP_REF AS_34	≤ 1 Stunde	≤ 4 Stunden
Deaktivierungen Nur während der Bürozeiten	54 55 56 56*b* 57	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_55_POS_PERIOD*** RT_25_TEL_IRI_CC	≤ 1 Stunde	≤ 1 Arbeitstag

	58	RT_26_EMAIL_IRI		
	59	RT_27_EMAIL_CC_IRI		
	67 Bst. c	EP_57_POS_PERIOD***		
	67 Bst. d	EP_36_RT_CC_IRI		
	67 Bst. e	EP_37_RT_IRI		

* FDA, ausgenommen FDA mit reduzierten Überwachungspflichten (Art. 51 VÜPF).

** Die AAKD mit weitergehenden Pflichten (Art. 22 und 52 VÜPF) sind davon ausgenommen.

*** Die AAKD mit weitergehenden Überwachungspflichten (Art. 52 VÜPF) sind davon ausgenommen.

**** AS_32_PREP_COV (Art. 64 VÜPF) ist während des Piketts nicht möglich (Art. 11 Abs. 1 Bst. d VÜPF).