Bern, 16.02.2022

Teilrevisionen vier Ausführungserlasse des BÜPF (VÜPF, GebV-ÜPF, VD-ÜPF, VVS-ÜPF)

Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens

Inhaltsverzeichnis

1 Ausgangslage

Anlässlich der Änderung vom 22. März 2019 des FMG[1] wurde ein Absatz 2 zu Artikel 2 des BÜPF[2] eingefügt. Dieser neue Absatz[3] ermächtigt den Bundesrat, die Kategorien von Mitwirkungspflichtigen (MWP) näher zu umschreiben, insbesondere jene nach Artikel 2 Buchstaben b, c und e BÜPF. Die Umsetzungsarbeiten richten sich auf die Teilrevisionen der VÜPF[4], was wiederum Teilrevisionen der GebV-ÜPF[5], der VD-ÜPF[6] und der VVS-ÜPF[7] nach sich zieht. Eine erste Ämterkonsultation wurde im März 2021 durchgeführt. Das Bundesgericht hat am 29. April 2021 ein Urteil[8] gefällt, in dem es eine Anbieterin als Anbieterin abgeleiteter Kommunikationsdienste (AAKD; Art. 2 Bst. c BÜPF) und nicht wie der Dienst ÜPF als Fernmeldedienstanbieterin (FDA; Art. 2 Bst. b BÜPF) einstufte. Um die Konsequenzen dieses Urteils auf die Praxis des Dienstes ÜPF gründlich zu analysieren, was einige Zeit in Anspruch nimmt, wurde entschieden, die Vorlagen in zwei Teilrevisionen zu trennen. Das erste vorliegende Revisionspaket (VÜPF, GebV-ÜPF, VD-ÜPF und VVS-ÜPF) beinhaltet nun alle Bestimmungen, die nicht die Definitionen der MWP regeln. Diese Bestimmungen, die die VÜPF an die 5G-Technologie anpassen, müssen zeitnah in Kraft treten. Die Definitionen der MWP (insb. Abgrenzung FDA AAKD) werden in einer zweiten Teilrevision angegangen.

Am 19. März 2021 hat das Parlament im Rahmen des Bundesgesetzes über administrative Erleichterungen und Entlastung des Bundeshaushalts eine Änderung des BÜPF beschlossen, welche die Bemessung der Entschädigungen und Kostenbeteiligungen einzelfallweise oder in Form von Pauschalen ermöglicht (Art. 38*a* BÜPF)[9]. Diese wird zu einer entsprechenden Änderung der GebV-ÜPF in einer separaten Vorlage führen.

1 Fernmeldegesetz vom 30.04.1997 (**FMG**; SR **784.10**)
2 Bundesgesetzes vom 18.03.2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (**BÜPF**, SR **780.1**; siehe AS **2020** 6181)
3 AS **2020** 6181. Der Bundesrat hat am 18.11.2020 entschieden, dass die Änderung vom 22.03.2019 des FMG am 01.01.2021 in Kraft tritt, ausser Art. 2 Abs. 1 Bst. b und 2 BÜPF, der zu einem späteren Zeitpunkt in Kraft gesetzt wird (AS **2020** 6178).
4 Verordnung vom 15.11.2017 über die Überwachung des Post- und Fernmeldeverkehrs (**VÜPF**, SR **780.11**)
5 Verordnung vom 15.11.2017 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (**GebV-ÜPF**, SR **780.115.1**)
6 Verordnung des EJPD vom 15.11.2017 über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (**VD-ÜPF**, SR **780.117**)
7 Verordnung vom 15.11.2017 über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (**VVS-ÜPF**, SR **780.12**)
8 2C_544/2020
9 BBl **2021** 669, S. 5/6

Zu erwähnen ist weiter das aktuelle Revisionspaket im Rahmen der Verordnung über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (VPMT)[10]. Die Möglichkeit mittels Mobilfunklokalisierung im Sinne von Artikel 23*q* nBWIS[11] den Standort und Aufenthalt einer betroffenen Person zu ermitteln, verlangt nach einer Anpassung der VÜPF, der GebV-ÜPF, der VD-ÜPF und der VVS-ÜPF. All diese Änderungen werden zu gegebener Zeit noch zu Koordinationsarbeiten mit der vorliegenden Vorlage führen.

2 Vorverfahren, insbesondere Vernehmlassungsverfahren

[*wird nach dem Vernehmlassungsverfahren ausgefüllt*]

Text …

3 Grundzüge der Vorlage

3.1 Anpassungen in der VÜPF

Die Technologie hat sich seit dem Inkrafttreten des BÜPF und seiner Ausführungserlasse am 1. März 2018 bereits weiterentwickelt. So ist die Mobilfunktechnologie zur fünften Generation (5G) übergegangen. Daher ist es erforderlich, die VÜPF an neue Identifikatoren (Adressierungselemente, Gerätenummern, Teilnehmernummern etc.) der 5G-Technologie und die Verwendung von temporären Identifikatoren anzupassen. Dies führt zur Schaffung von zwei neuen Auskunftstypen IR_53_ASSOC_PERM (Auskünfte über längerfristig zugeordnete Identifikatoren) im neuen Artikel 48*a* und IR_54_ASSOC_TEMP (sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren) im neuen Artikel 48*b*.

Im Rahmen dieser Revision werden noch drei weitere Auskunftstypen geschaffen:

- Der Auskunftstyp IR_51_EMAIL_LAST, Auskünfte über E-Mail-Dienste (Art. 42*a*), der den Zeitpunkt der letzten zugriffsrelevanten Aktivität eines E-Mail-Dienstes liefert. Dies dient zur Bestimmung des Zeitpunkts, wann ein Kommunikationsvorgang abgeschlossen ist.

10 Vernehmlassungen =>Laufende Vernehmlassungen =>EJPD =>Teilinkraftsetzung des Bundesgesetzes über polizeiliche Massnahmen zur Bekämpfung von Terrorismus; Verordnung über polizeiliche Massnahmen zur Bekämpfung von Terrorismus =>Vernehmlassungsvorlage betr. VD-ÜPF und Vernehmlassung-2 (VPMT) betr. VÜPF (S. 12), GebV-ÜPF (S. 14) und VVS-ÜPF (S. 15)

11 In der Vorlage des Bundesgesetzes vom 25.09.2020 über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (**PMT**; BBl **2020** 7747)

- Der Auskunftstyp IR_52_COM_LAST, Auskünfte über andere Fernmelde- oder abgeleitete Kommunikationsdienste (Art. 43*a*), der Angaben über die letzte zugriffsrelevante Aktivität eines anderen Fernmelde- oder abgeleiteten Kommunikationsdienstes liefert.
- Der Auskunftstyp IR_55_TEL_ADJ_NET, Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten (Art. 48*c*), der spezifische Probleme der Identifikation der Täterschaft löst, wie sie bei gefälschter (Spoofing) oder unbekannter Telefonnummer des Anrufers auftreten.

Um die neuen technischen Möglichkeiten des «Lawful Access to Location Services» (LALS) zur Positionsbestimmung im Mobilfunk zu nutzen, werden vier neue Überwachungstypen geschaffen. 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 Abs. 1 Bst. b und c).

Weiter zu erwähnen ist der neue Artikel 4*a* (Beginn und Ende der rückwirkenden Überwachung), der die in der Praxis umstrittene Berechnung der Frist von sechs Monaten neu regelt. Artikel 20 (Erfassung von Angaben zur Person bei Mobilfunkdiensten) wird ergänzt und neu strukturiert in Bestimmungen für natürliche Personen (Art. 20*a*) und juristische Personen (Art. 20*b*). Artikel 20*a* Absatz 5 sieht neu eine Ausnahme zur Identitätsprüfung und Erfassung der Angaben für Polizeibehörden, den Nachrichtendienst des Bundes (NDB) und weitere Personengruppen vor, sofern eine gesetzliche Grundlage vorhanden ist, welche ihnen erlaubt, ihre wahre Identität nicht preisgeben zu müssen.

Dazu werden punktuelle Änderungen in verschiedenen Bestimmungen angebracht und der Anhang mit neuen Begriffen und Abkürzungen ergänzt.

3.2 Anpassungen in der GebV-ÜPF

Infolge der Einführung der oben erwähnten fünf Auskunfts- und vier Überwachungstypen in die VÜPF wird auch der Anhang der GebV-ÜPF entsprechend angepasst. Die Gebühren und Entschädigungen der anderen Auskunfts- und Überwachungstypen bleiben unverändert.

Weiter gibt es punktuellen Änderungen in den Artikeln 3, 15, 17 Absatz 3, 18 und 19 Absatz 1 GebV-ÜPF.

3.3 Anpassungen in der VD-ÜPF

Neu gilt die VD-ÜPF nicht nur für die MWP, sondern auch für die Behörden gemäss Artikel 1 Absatz 2 Buchstaben a-f VÜPF. Entsprechend wird auch Artikel 3 VD-ÜPF geändert, der die gesicherte Kommunikation regelt.

Infolge der Einführung der oben erwähnten Auskunftstypen in die VÜPF werden auch die Bearbeitungsfristen für die Lieferung von Auskünften in Artikel 14 VD-ÜPF entsprechend angepasst.

In der Praxis wurde die Frist von einem Arbeitstag im bisherigen Artikel 14 Absatz 2 Buchstabe b VD-ÜPF von den auskunftsberechtigten Behörden als zu lange erachtet. Dies insbesondere dann, wenn ihre Anfrage an einem Wochenende oder an einem Feiertag gestellt wurde und die Auskunft dringend war. Aus diesem Grund wird für die «grossen» FDA und AAKD für Auskunftsgesuche ausserhalb der Normalarbeitszeiten und an Feiertagen (Pikett) 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. 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 damit die Strafverfolgung nicht behindert werden.

Auch in Artikel 14 Absatz 3 wurde die Frist für die „kleinen" MWP im Vergleich zum bisherigen Recht für die einfachen Auskünfte von zwei auf einen Arbeitstag reduziert, um dem dringenden Bedürfnis der Strafverfolgungsbehörden nach kürzeren Fristen Rechnung zu tragen.

Weiter gibt es punktuelle Änderungen in den Artikeln 10 Absatz 4 (neu), 11 Absatz 2, 12 sowie 18 Absatz 2 und 3 VD-ÜPF.

3.4 Anpassungen in der VVS-ÜPF

Mit der vorliegenden Vorlage wird die Gelegenheit genutzt, auch die VVS-ÜPF teil zu revidieren. Neben den Zugriffen auf die Anzeige der Betriebslage der Teile des Verarbeitungssystems, auf welche die Person Zugriff hat (PTSS-Dashboard), welche den Zustand der Überwachungskomponenten visualisiert, werden neu 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) geregelt. Weiter wird Artikel 3 Absatz 2 Buchstaben a-c mit dem 1. Abschnitt des 3. Kapitels der VÜPF ergänzt, da insbesondere auch die besonderen Auskünfte und Überwachungen (Art. 25) wie auch die Auskunftstypen mit flexibler Namenssuche (Art. 27) darunter fallen (vgl. Ziff. 5.4). Ebenso wird ein Begriff in Artikel 11 angepasst.

4 Auswirkungen für Bund, Kantone und MWP

Die vorgesehenen Anpassungen der vier Verordnungen (VÜPF, GebV-ÜPF, VD-ÜPF und VVS-ÜPF) sollten aus heutiger Sicht keine erheblichen finanziellen und personellen Auswirkungen haben, weder für Bund und Kantone, noch für die MWP. Trotzdem sind folgende minimale finanziellen Auswirkungen zu erwähnen:

- Die neuen Auskunfts- und Überwachungstypen und die Anpassungen an die 5G-Technologie in der VÜPF können für die MWP finanzielle und wirtschaftliche Konsequenzen haben, je nachdem, welche technischen Anpas-

sungen sie an ihren Systemen infolge dieser Teilrevisionen vornehmen müssen. Insbesondere für die Realisierbarkeit der neuen Auskunfts- und Überwachungstypen werden die MWP Investitionskosten haben. Die Strafverfolgungsbehörden beteiligen sich mit den Entschädigungen an den Betriebskosten der MWP.

- 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 bestehenden Mitteln aufgefangen werden können.
- Die neuen Auskunfts- und Überwachungstypen werden voraussichtlich relativ selten beziehungsweise viel weniger als die anderen Auskunfts- und Überwachungstypen genutzt. Es ist daher mit einer eher geringen Zusatzbelastung der Budgets der Kantone zu rechnen. Die Gebühren der neuen Typen bewegen sich im Rahmen der bereits bestehenden Auskunfts- und Überwachungstypen. Wie gross die Belastung der kantonalen Strafverfolgungsbehörden effektiv sein wird, hängt von der Anzahl Anordnungen dieser Typen ab, die weder voraussehbar noch beeinflussbar ist.
- Deshalb sollte insgesamt auch der Kostendeckungsbeitrag des Bundes mit den neu vorgesehenen Gebühren und Entschädigungen unverändert bleiben.
- Gemäss dem neuen Artikel 15 Absatz 2 GebV-ÜPF kann der Bund den MWP, die selber nicht zur Erteilung von Auskünften oder zur Durchführung von Überwachungen verpflichtet sind und den Dienst ÜPF dabei unterstützen, ebenfalls eine Entschädigung entrichten. Diese neue Bestimmung wird kaum finanzielle Auswirkungen für die MWP und den Bund haben, da diese Konstellation sich eher selten in der Praxis realisiert.

5 Erläuterungen zu einzelnen Artikeln

5.1 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, optionale Funktionen, bestimmte Technologien oder Funktionen oder bestimmte Standards respektive bestimmte 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 Mitwirkungspflichten eine ausführliche Begründung zu liefern, warum bestimmte Parameter, Daten und Funktionen nicht vorhanden sind respektive nicht geliefert werden können.

Ersatz von Ausdrücken

Absatz 1: In der Praxis hat sich gezeigt, 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. Der Begriff «WLAN-Zugangspunkt» wird daher an den entsprechenden Stellen durch den allgemeineren Begriff «WLAN-Zugang» ersetzt, da dieser sowohl Zugangspunkte als auch Hotspots einschliesst.

Absatz 2: Die Überarbeitung wird zum Anlass genommen, in der VÜPF die Abkürzung *AAKD* aufzunehmen, die bereits in der Praxis zusammen mit der Abkürzung *FDA* verwendet wird (s. auch die Änderung in Art. 1 Abs. 2 Bst. j).

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 einerseits eine unnötige Wiederholung des Gesetzestextes in der Verordnung zu vermeiden und da andererseits ein neuer Artikel (Art. 2*b*) zur näheren Umschreibung der Kategorie *AAKD* geschaffen wird. 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 bestimmt, sondern durch das EJPD, und zwar in Artikel 3 VD-ÜPF (Departementsverordnung).

Die *Buchstaben b* und *c* enthalten 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 sechs Monate rückwirkend verlangt werden (Art. 273 Abs. 3 StPO[12]). Dafür müssen die 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. 2 VÜPF i. V. m. Art. 21 Abs. 2 und Art. 22 Abs. 2 BÜPF) während sechs Monaten aufbewahren. Was die Frist von sechs 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 zu Diskussionen geführt hat.

Im neuen *Absatz 1* wird der «dies a quo» für die Berechnung der Frist von sechs Monaten für rückwirkende Überwachungen festgelegt. Dieser Tag entspricht dem Tag des Empfangs der Anordnung durch den Dienst ÜPF. Somit ist nicht das Datum der Anordnung oder der Übermittlung[13] durch die anordnende Behörde massgebend.

Für die Berechnung der Frist von sechs Monaten wird der Zeitpunkt des Empfangs demjenigen der Übermittlung der Anordnung aus nachfolgenden Gründen vorgezogen: Bei einer Übermittlung über das WMC[14], welche den Normalfall darstellt, macht es keinen Unterschied, ob die Berechnung der Frist auf den Zeitpunkt 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, 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). Problematisch ist dieser Zeitabstand, da die Anbieterinnen auch verpflichtet sind, die historischen Daten zu löschen. Im Beispiel 4 wäre das Risiko somit grösser, dass die von den anordnenden Behörden verlangten Daten durch die Anbieterinnen bereits gelöscht sind. Mit der Wahl des Zeitpunkts des Empfangs kann somit die Zeit zwischen dem Eingang der Anordnung beim Dienst ÜPF und dem Auftrag an die Anbieterinnen möglichst kurzgehalten werden.

12 Schweizerische Strafprozessordnung vom 05.10.2007 (Strafprozessordnung, **StPO**; SR **312.0**)

13 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).

14 Warrant Management Component (WMC): Eine Komponente des Verarbeitungssystems FMÜ, in Betrieb seit dem 18.03.2019.

Zu beachten ist, dass mit dem Tag der Übermittlung 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[15].

Falls die Anordnung im Verarbeitungssystem des Dienstes ÜPF (WMC) hochgeladen wird, gilt dieser Zeitpunkt als Tag der Übermittlung und des Empfangs durch den Dienst ÜPF (s. u. Bsp. 2). Bei telefonischer Beauftragung gilt der Zeitpunkt des Anrufs und nicht der Zeitpunkt des Empfangs der schriftlich nachgereichten Anordnung (s. u. Bsp. 3).

Die Überwachung beginnt somit frühestens sechs Monate vor dem Tag des Empfangs durch den Dienst ÜPF. Der früheste Beginn der Überwachung ist um Mitternacht (00.00 Uhr und 0 Sekunden[16], Schweizer Zeit) am Beginn dieses Tages. Zur Erinnerung Artikel 273 Absatz 3 StPO sieht eine Frist in Monaten und nicht in Stunden vor.

Die Berechnung der Frist von sechs Monaten richtet sich nach der Lehre[17] und der Rechtsprechung[18]: «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.»[19] 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 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, wird im *zweiten Satz* geregelt. Wenn beispielsweise die Anordnung 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. Wenn es aber diesen Tag (31.) im Monat des Beginns der Überwachung (sechs Monate zurückgerechnet) nicht gibt (z. B. keinen 31. April), dann nimmt man den letzten existierenden Tag dieses Monats (30. April, s. unten die Beispiele 2-3).

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[20] Schweizer Zeit dieses Tages (s. u. Bsp. 1-4). Wird die

15 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»)

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

17 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.

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

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

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

rückwirkende Überwachung 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 angefallenen Daten. Es erfolgt somit keine zweite nachträgliche Datenlieferung der restlichen Daten (Randdaten, 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 Daten bei der Anbieterin aufgrund von üblichen Verzögerungen erst später verfügbar sind (beispielsweise Daten aus dem Roaming), müssen diese ebenfalls nicht nachgeliefert werden. Falls diese Daten 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).

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 (s. u. Erläuterungen zu Art. 21 Abs. 4 VÜPF) zu berücksichtigen. Die Anbieterin führt die rückwirkende Überwachung innerhalb von 3 Arbeitstagen aus, bei dringenden Fällen innerhalb von 6 Stunden (Art. 17 Abs. 3 VD-ÜPF).

Anbei werden einige Beispiele für die Berechnung der Frist von sechs Monaten aufgeführt. Dabei gibt es anzumerken, dass die Uhrzeit des Beginns der Überwachung standardmässig 00.00 Uhr und 0 Sekunden und die Uhrzeit des Endes der Überwachung standardmässig 23.59 Uhr und 59 Sekunden ist. Eine Ausnahme besteht, wenn die Ausführung noch am Tag der Anordnung stattfindet. Dann ist die Uhrzeit des Endes gleich der Uhrzeit der Ausführung plus 59 Sekunden. Es sind die im Moment der Ausführung vorhandenen Daten zu liefern.

Beispiel 1: Anordnung datiert vom Dienstag 10.11.2020, mittels verschlüsseltem Mail am Donnerstag **12.11.2020** um 9.00 Uhr vom Dienst ÜPF erhalten
→ Beginn **TT = 12**, MM: 11 - 6 = 5 → **MM = 5**, **JJJJ = 2020**
Frühestmöglicher Beginn ist der 12.05.2020, 00.00 Uhr;
spätestmögliches Ende ist der 12.11.2020, 23.59 Uhr.

Beispiel 2: Anordnung hochgeladen in WMC am Montag, **31.08.2020,** um 18.00 Uhr
→ Beginn **TT = 31**, MM: 8 – 6 = 2 → **MM = 02**, **JJJJ = 2020**
Den 31.02.2020 gibt es nicht, also wird auf den letzten Tag des Februars in 2020 «abgerundet».
Frühestmöglicher Beginn ist der 29.02.2020, 00.00 Uhr;
spätestmögliches Ende ist der 31.08.2020, 23.59 Uhr.

Beispiel 3: Mündliche Anordnung per Telefon an den Dienst ÜPF am Sonntag **31.05.2020** um 16.50 Uhr
→ Beginn **TT = 31**, MM: 5 - 6 = -1 + 12 → **MM** = **11** des Vorjahres, JJJJ: 2020 - 1 → **JJJJ = 2019**
Den 31.11.2019 gibt es nicht, also wird auf den letzten Tag des Novembers in 2019 «abgerundet».
Frühestmöglicher Beginn ist der 30.11.2019, 00.00 Uhr;
spätestmögliches Ende ist der 31.05.2020, 23.59 Uhr.

Beispiel 4: Anordnung datiert vom Mittwoch, 08.04.2020, per Post am Donnerstag, 09.04.2020, (Poststempel) geschickt, keine telefonische Avisierung. Im Dienst ÜPF am Dienstag (nach Ostermontag), **14.04.2020**, um 9.00 Uhr erhalten. Überwachungsauftrag am 14.04.2020 um 9.50 Uhr an die Anbieterinnen weitergeleitet.
→ Beginn **TT = 14**, MM: 4 - 6 = -2 + 12 → **MM** = **10** des Vorjahres, JJJJ: 2020 - 1 → **JJJJ = 2019**
Frühestmöglicher Beginn ist der 14.10.2019, 00.00 Uhr;
spätestmögliches Ende ist der 14.04.2020, 23.59 Uhr.
Bemerkung: Bei telefonischer Anordnung gilt der Tag des Anrufs als Stichtag, nicht der Tag des Empfangs der schriftlichen Bestätigung (s. Bsp. 3).

Beispiel 5: Anordnung einer dringenden rückwirkenden Überwachung, hochgeladen im WMC durch die anordnende Behörde am Freitag, **28.08.2020**, **um 16.00 Uhr**, beauftragt an die MWP durch den Dienst ÜPF um 16.30 Uhr.
→ Beginn **TT = 28**, MM: 8 - 6 = 2 → **MM = 02**, **JJJJ = 2020**
Frühestmöglicher Beginn ist der 28.02.2020, 00.00 Uhr;
spätestmögliches Ende ist der 28.08.2020.

Die Uhrzeit bestimmt sich 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 Randdaten 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.

Art. 11 Leistungen ausserhalb der Normalarbeitszeiten und an Feiertagen

Diese Bestimmung regelt die Leistungen des Dienstes ÜPF sowie der genannten MWP ausserhalb der Normalarbeitszeiten, d. h. 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.

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, ausser jene mit reduzierten Überwachungspflichten gemäss Artikel 51, und die AAKD mit weitergehenden Überwachungspflichten (Art. 52) haben alle Pikettleistungen nach Absatz 1 Buchstaben a–e zu erbringen. Dagegen müssen keinen Pikettdienst leisten: 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.

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 der genannten standardisierten Auskünfte geregelt. In *Buchstabe b* werden weitere standardisierte Auskünfte aufgeführt. In *Buchstabe c* ist geregelt, welche Typen von Echtzeitüberwachungen im Pikett aktiviert werden. In *Buchstabe d* ist festgelegt, welche Typen von als dringend erklärten rückwirkenden Überwachungen im Pikett durchgeführt werden. In *Buchstabe e* sind die Typen von Notsuchen und Fahndungen aufgeführt, die im Pikett durchgeführt werden.

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.

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

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 ausgeführt.

Artikel 18 Absatz 1 legt den Grundsatz fest, wonach folgende Kategorien von MWP die Auskünfte über die Abfrageschnittstelle des Verarbeitungssystems des Dienstes ÜPF (IRC[21]) zu erteilen haben:

- die FDA, mit Ausnahme von denjenigen mit reduzierten Überwachungspflichten (Art. 51),

21 IRC: Information Request Component des Verarbeitungssystems des Dienstes ÜPF; in Betrieb seit dem 18. März 2019.

- die AAKD mit weitergehenden Auskunftspflichten (Art. 22) und
- die AAKD mit weitergehenden Überwachungspflichten (Art. 52);

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 der MWP angebotenen Dienste.

In *Absatz 2* 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 oder automatisierter Erteilung haben. Die Pflicht zur Automatisierung betrifft häufige, zeitkritische oder einfache Auskünfte. Die Wahlmöglichkeit zwischen automatisierter und manueller Auskunftserteilung 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. Diese Wahlmöglichkeit führt dazu, dass einige MWP Auskünfte eines bestimmten Typs manuell erteilen, während andere MWP die Auskünfte des gleichen Typs automatisiert erteilen. Von den fünf neuen Auskunftstypen müssen die Auskünfte gemäss Artikel 42*a* (IR_51_EMAIL_LAST), 43a (IR_52_COM_LAST), 48*a* (IR_53_ASSOC_PERM) und 48*b* (IR_54_ASSOC_TEMP) automatisiert erteilt werden, während bei der Auskunft gemäss Artikel 48*c* (IR_55_TEL_ADJ_NET) die Wahl zwischen manueller oder automatisierter Erteilung besteht. Die automatisierte Auskunftserteilung läuft ohne menschliche Mitwirkung des Dienstes ÜPF und der MWP ab; die berechtigte Behörde gibt ihr Auskunftsgesuch in die Auskunftsgesuchskomponente IRC des Verarbeitungssystems 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 Mitarbeiterin oder der Mitarbeiter der MWP meldet sich in der IRC an und füllt dort von Hand die entsprechende Antwortmaske aus. Die berechtigte Behörde erhält die Antwort ebenfalls in der IRC. Bei der manuellen Erteilung der Auskunft ausserhalb des Verarbeitungssystems gibt die berechtigte Behörde ihr Auskunftsgesuch in die IRC ein, der Dienst ÜPF übermittelt dieses jedoch 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 sieht vor, dass die AAKD mit weitergehenden Auskunftspflichten (Art. 22) von der Auskunftserteilung nach Artikel 48*b* befreit sind. Die Umsetzung dieses in Echtzeit zu beantwortenden Auskunftstyps erfordert Investitionen der betreffenden MWP in eine neue Anfrageschnittstelle und in das System zur automatisierten Auskunftserteilung. Aufgrund der Verhältnismässigkeit sollen diese Zusatzbelastungen nur den «grossen» FDA und den «grossen» AAKD (Art. 52) auferlegt werden. Weiter sieht Absatz 3 vor, dass die AAKD mit weitergehenden Auskunftspflichten (Art. 22) bei Auskünften gemäss den Artikeln 38, 39 und 48*c* nur die ihnen vorliegenden Infor-

mationen liefern, da sie gemäss Artikel 21 Absatz 6 Buchstaben b und c nicht verpflichtet sind, die entsprechenden Randdaten aufzubewahren. Während der Normalarbeitszeiten müssen sie und während des Pikettdienstes (Art. 11) dürfen sie diese Auskünfte erteilen.

Absatz 4 betrifft die Auskunftserteilung der FDA mit reduzierten Überwachungspflichten (Art. 51). Auch sie sind von der Auskunftserteilung nach Artikel 48*b* aus den gleichen Gründen (s. Erläuterungen zu Abs. 3) befreit. Die Mindestanforderung ist die manuelle Auskunftserteilung ausserhalb des Verarbeitungssystems (s. Erläuterungen zu Abs. 2). Es besteht jedoch auch die Möglichkeit der manuellen Auskunftserteilung über das Verarbeitungssystems (IRC, s. Erläuterungen zu Abs. 2). Eine FDA mit reduzierten Überwachungspflichten (Art. 51) kann weiterhin auch den Wunsch äussern, bestimmte Auskünfte automatisiert zu erteilen. Der Dienst ÜPF entscheidet dann nach Absprache, ob dies in der IRC umgesetzt werden kann.

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 18*a* regelt die Pflichten für die Lieferung von Auskünften durch die AAKD ohne weitergehende Pflichten, d.h. 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 Übergangsmittels.

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

Art. 18b Beizug Dritter bei der Auskunftserteilung

Im zur besseren Lesbarkeit neu eingefügten Artikel 18b wird die Regelung des bisherigen Artikels 18 Absatz 1 2. Satz und Absatz 4 2. Satz, wonach die MWP Dritte zur Auskunftserteilung beziehen können, übernommen.

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

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*, stützen 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 Teilnehmerin oder den Teilnehmer 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 (Bst. a) und bei juristischen Personen deren Angaben (Bst. b) überprüfen.

Unter Aktivierung beziehungsweise Freischaltung ist der Zeitpunkt zu verstehen, ab dem eine Teilnehmerin oder ein Teilnehmer den entsprechenden Dienst nutzen kann. 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, d. h. 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 respektive die Überprüfung der Angaben der juristischen Person durch die professionellen Wiederverkäuferinnen (Art. 2 Bst. f BÜPF) vorzunehmen ist, falls die Abgabe des Zugangsmittels oder die erstmalige Aktivierung unmittelbar durch diese erfolgt. Zum Beispiel nimmt bei der Abgabe des Zugangsmittels in einem Shop einer professionellen Wiederverkäuferin diese die Identifizierung der oder des Teilnehmenden vor, kopiert deren oder dessen 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. In diesem Fall

muss die FDA keine zusätzliche Überprüfung der Angaben zur Person vornehmen. Die ordnungsgemässe Registrierung und Identifizierung der oder des Teilnehmenden durch die professionelle Wiederverkäuferin sowie die Weiterleitung der Angaben an die FDA ist durch die FDA in geeigneter Weise zu überprüfen und durchzusetzen. 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[22]. 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).

22 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.

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[23]. In diesem Fall sind die Sicherheits- und Qualitätsstandards des FINMA-Rundschreibens 2016/7 «Video- und Online-Identifizierung»[24] 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 (Transliteration), können sie direkt für die normale, d. h. 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.

23 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**)

24 finma.ch =>Dokumentation => Rundschreiben

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, z. B. 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).

Absatz 4, erster Satz, verlangt, dass das vorgelegte Ausweisdokument 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 3 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 Kopie zur FDA weiterleiten. Die Frist wird auf 14 Tage festgelegt, damit sie auch für kleinere professionelle Wiederverkäuferinnen zumutbar ist. Mit diesem Absatz sollen die Verantwortlichkeiten klarer abgegrenzt werden (s. a. die entsprechende Strafbestimmung in Art. 39 Abs. 1 Bst. c BÜPF).

Absatz 5 sieht neu eine Ausnahme zur Identitätsprüfung und Erfassung der Angaben einerseits für Polizeibehörden und den Nachrichtendienst des Bundes (NDB) vor, sofern eine gesetzliche Grundlage vorhanden ist, welche ihnen erlaubt, ihre wahre Identität nicht preisgeben zu müssen. Andererseits gilt diese Ausnahme auch für weitere Personengruppen, sofern auch hier eine gesetzliche Grundlage vorhanden ist, welche ihnen erlaubt, ihre wahre Identität nicht preisgeben zu müssen. Diese Ausnahme kann von den Polizeibehörden von Bund und Kantonen sowie dem NDB verlangt werden.

Die Identitätsprüfung nach Absatz 1 war nach bisherigem Recht für alle Teilnehmenden vorgesehen, so auch für Angehörige der Polizeibehörden und Mitarbeitende des NDB. Diese Regelung hat sich in den letzten Jahren in der Praxis für diese Behörden

als besonders problematisch erwiesen. Bei den FDA und den professionellen Wiederverkäuferinnen hat eine grosse und nicht kontrollierbare Anzahl an Personen Zugriff auf die Systeme und somit auf die Daten, welche zur Erteilung der Auskünfte benötigt werden. Aus diesem Grund ist der Schutz der Identität der Teilnehmenden im heutigen System ungenügend, insbesondere wenn es sich um Angehörige der Polizeibehörden und Mitarbeitende des NDB handelt.

Verdeckte Fahnderinnen und Fahnder (Art. 298*a* ff. StPO) haben die gesetzliche Aufgabe, Verbrechen und Vergehen aufzuklären. Um dieses Ziel zu erreichen, dürfen sie Scheingeschäfte abschliessen oder den Willen zum Abschluss vortäuschen (Art. 298*a* Abs. 1 StPO). Das Gesetz sieht vor, dass die wahre Identität und die Funktion von verdeckten Fahnderinnen und Fahndern während der Einsatzzeit nicht erkennbar sein sollen. Die Bekanntgabe der Identität einer verdeckten Fahnderin oder eines verdeckten Fahnders kann nicht nur die Ziele ihrer Aufgabe (Entdeckung von schweren Straftaten) zuwiderlaufen, sondern erhebliche Gefahren für Leib und Leben der Polizistin oder des Polizisten darstellen, insbesondere in den Fällen, bei denen hinter den Delikten eine kriminelle Organisation im Sinne von Artikel 260ter StGB steht. Die geltenden Sicherheitslücken bei den Zugriffsbefugnissen der FDA führen allerdings genau zu solchen gefährlichen Situationen.

Verdeckte Ermittler (Art. 151 und 285*a* ff. StPO) werden mit einer Legende ausgestattet. Im Gegensatz dazu dürfen verdeckte Fahnder nicht mit einer Legende ausgestattet werden (Art. 298*a* Abs. 2 StPO); dies aus Überlegungen der Verhältnismässigkeit, da die verdeckte Ermittlung nur zur Aufdeckung von besonders schweren Delikten, die in Artikel 286 Absatz 2 StPO klar festgehalten sind, anwendbar ist.

Mitarbeitende des NDB sind in verschiedenen Funktionen in Situationen tätig, bei denen das Bekanntwerden ihrer echten Identität und ihrer Zugehörigkeit zum NDB zu einer direkten Bedrohung ihrer persönlichen Integrität, derer von Personen ihres Umfelds oder zur Gefährdung ihrer Auftragserfüllung führen kann. Dies einerseits, indem sie direkt durch von ihnen kontaktierte Personen bedroht werden können. Andererseits können ihnen bei einer Arbeit im Rahmen der Spionageabwehr Nachteile bis hin zur Verhaftung erwachsen, wenn sie später in ein Land einreisen, gegen das sich die Abwehrtätigkeit des NDB gerichtet hat.

Mitarbeitende des NDB sind namentlich bei der Rekrutierung und Führung von Informanten auf die Verwendung von anonymisierten, immer wieder wechselnden oder nur einmal benützten Mobiltelefonanschlüssen angewiesen. Deren Inhaber dürfen nicht einfach identifizierbar sein. Auch bei der Observation von Personen im nachrichtendienstlichen Umfeld muss der NDB die verwendeten Kommunikationsanschlüsse regelmässig austauschen, um die Erkennbarkeit zu verringern. Die Gegenseite kann hier - illegal - sogenannte IMSI-Catcher verwenden und bei auffälligen Mobiltelefonen versuchen, die Inhaber zu identifizieren.

Die gesetzlich vorgesehene Möglichkeit des NDB, unter Tarnidentitäten zu arbeiten, reicht hierbei für die Beschaffung der in grösserer Anzahl benötigten anonymisierten Mobiltelefonanschlüsse nicht aus. Der NDB muss die Möglichkeit haben, von den Mobiltelefonprovidern in ausreichender Anzahl anonymisierte Mobiltelefonanschlüsse zu beziehen, das heisst bis zu mehreren hundert pro Jahr. Tarnidentitäten sind

nach Artikel 18 NDG nicht nur für Angehörige des NDB sondern auch für Mitarbeitende der kantonalen Vollzugsbehörden und unter bestimmten Umständen auch für Quellen des NDB vorgesehen.

Nicht alle FDA können heute mit ihren aktuellen Systemen sicherstellen, dass diese nicht durch Kriminelle ausgenützt werden, um verdeckte Fahnder zu identifizieren und ihr Leben und ihre Aufgabe zu gefährden. Deshalb ist es nötig, dass die FDA bestrebt sind, technische Lösungen zu implementieren, damit die Polizeibehörden und die Mitarbeitenden des NDB in der Erfüllung ihrer Aufgaben nicht behindert oder sogar gefährdet werden. Auch ein fehlender Ausweis der oder des Teilnehmenden im System der FDA lässt heute teilweise den Schluss zu, dass es sich um eine Mitarbeiterin oder einen Mitarbeiter einer Sicherheitsbehörde handelt.

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. 21 Aufbewahrungsfristen

Dieser Artikel wurde umfassend überarbeitet, um die Regelungen der Aufbewahrungsfristen für die einzelnen Datenkategorien besser zu strukturieren, zu ergänzen und zu präzisieren. Für AAKD, die sowohl weitergehende Auskunftspflichten (Art. 22) als auch weitergehende Überwachungspflichten (Art. 52) haben, wird die für die vorliegende Revision gewählte kompakte Schreibweise *AAKD mit weitergehenden Pflichten* verwendet. Die prinzipiellen Aufbewahrungsfristen werden nicht geändert, das heisst Bestandsdaten (subscriber data) sind wie bisher während der Dauer der Kundenbeziehung sowie während 6 Monaten nach deren Beendigung (Abs. 1 und 3), nutzungsabhängige Daten (usage data) sind während 6 Monaten (Abs. 2 und 4) und Identifikationsdaten der Endbenutzenden von professionell betriebenen öffentlichen WLAN-Zugängen sind während der Dauer der Zugangsberechtigung sowie während 6 Monaten nach deren Ende aufzubewahren (Abs. 5).

Neu hinzugefügt wurden in *Absatz 1* die Angaben über längerfristig zugeordnete Identifikatoren gemäss Artikel 48*a*.

Absatz 2 ist ebenfalls neu und regelt die Aufbewahrungsfrist für die nutzungsabhängigen Daten über die letzte zugriffsrelevante Aktivität bei E-Mail-Diensten sowie anderen Fernmelde- oder abgeleiteten Kommunikationsdiensten, die für die neu geschaffenen Auskunftstypen nach den Artikeln 42*a* und 43*a* benötigt werden.

Die bisherige allgemeine Bezeichnung *Angaben zum Zweck der Identifikation* wird neu in den einzelnen Absätzen jeweils präzisiert. Meist handelt es sich dabei um Bestandsdaten (Abs. 1 und 3). In bestimmten Fällen kann es sich jedoch auch um nutzungsabhängige Daten handeln (Abs. 2, 4 und 5). Aufgrund der Präzisierung der *Angaben zum Zweck der Identifikation* wurde *Absatz 3* neu hinzugefügt, um im Mobilfunkbereich die Aufbewahrungsfrist für die Angaben über die Teilnehmenden und für die Kopie des Identitätsnachweises explizit zu regeln. Dazu 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 geregelt.

Bisher waren die Daten über die Zuteilung und Übersetzung von IP-Adressen und Portnummern im bisherigen Absatz 2 Buchstabe b gemeinsam enthalten. Neu werden sie getrennt geregelt nach eindeutiger und mehrdeutiger Zuteilung: Daten über die eindeutige Zuteilung von IP-Adressen im neuen *Absatz 4* und Daten über die mehrdeutige Zuteilung und Übersetzung (NAT) von IP-Adressen und Portnummern im neuen *Absatz 6 Buchstabe b*. Innerhalb der eindeutig zugeteilten IP-Adressen ist zwischen fest zugeteilten (fixen) und dynamisch zugeteilten IP-Adressen zu unterscheiden. Die Aufbewahrungsfrist für Daten über die Zuteilung von fixen IP-Adressen umfasst, wie bei allen Bestandsdaten, die gesamte Dauer der Kundenbeziehung zuzüglich 6 Monate. Bei den dynamisch zugeteilten IP-Adressen beträgt die Aufbewahrungsfrist der Zuteilungsdaten jedoch nur 6 Monate, da sie zu den nutzungsabhängigen Daten gehören.

Der Wortlaut des *Absatzes 5* entspricht dem zweiten Satz des bisherigen Absatzes 1 und wird lediglich redaktionell angepasst («WLAN-Zugang» statt «WLAN-Zugangspunkt»; s. Erläuterungen zum Ersatz von Ausdrücken, Abs. 1).

Bei den Daten nach *Absatz 6* handelt es sich um Daten zur Identifikation nach Artikel 22 Absatz 2 2. Satz BÜPF. *Absatz 6* baut auf dem bisherigen Absatz 2 auf und wurde um *Buchstabe c* ergänzt, der die Aufbewahrungsfrist für die Randdaten zur Bestimmung der unmittelbar benachbarten Netze für die Auskünfte gemäss Artikel 48*c* regelt (s. die dortigen Erläuterungen). Durch den Entfall des Wortes *liefern* wird klargestellt, dass diese Daten zur Identifikation aufzubewahren, aber im Rahmen von Auskünften nicht zu liefern sind, sofern es sich bei ihnen um Randdaten handelt. Solche Randdaten sind hier von den MWP lediglich zur Identifikation der Benutzerschaft auszuwerten und es sind die gemäss Auskunftsgesuch geforderten Angaben zu liefern. Die Randdaten selbst 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.

Absatz 7 entspricht dem bisherigen Absatz 3 mit der nötigen Anpassung des Verweises auf den Absatz 6 (statt Abs. 2) und regelt weiterhin die Vernichtung der Randdaten, die dort näher umschrieben sind.

Hinweis: Über kurzzeitig zugeordnete Identifikatoren gemäss Artikel 48*b* müssen keine Angaben aufbewahrt werden. Abfragen dieses Auskunftstyps sind aufgrund des sehr dynamischen Ablaufs dieser Zuordnungen nur in Echtzeit möglich (s. Erläuterungen zu Art. 48*b*).

Art. 26 Auskunftstypen im Allgemeinen

Absatz 1 wird zum einen formell umstrukturiert. Auf die Nummerierung in Ziffern wird zugunsten einer neu etwas umfangreicheren Aufzählung in Buchstaben verzichtet. Zum andern werden die vier neuen Auskunftstypen in diese Auflistung der verschiedenen Auskunftstypen aufgenommen. *Buchstabe b* wird mit Artikel 42*a* (IR_51_EMAIL_LAST, Auskünfte über E-Mail-Dienstes) und mit Artikel 43*a* (IR_52_COM_LAST, Auskünfte über abgeleitete Kommunikationsdienste) ergänzt. Im neuen *Buchstaben h* werden die Artikel 48*a* (IR_53_ASSOC_PERM, Auskünfte über längerfristig zugeordnete Identifikatoren) und Artikel 48*b* (IR_54_ASSOC_TEMP, sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren) genannt und im neuen *Buchstabe i* der Arikel 48*c* (IR_55_TEL_ADJ_NET, Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten). Ausserdem wird in *Buchstabe d* der spezifische Begriff «Ausweiskopie» durch den allgemeineren Begriff «Identitätsnachweis» ersetzt, da neu auch elektronische Identitäten verwendet werden können.

In *Absatz 2* wird eine redaktionelle Änderung vorgenommen. Die Verwendung des Begriffs «Mitwirkungspflichtige» 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 subsummiert. 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 und Fahndung, zwei zur Notsuche) ergänzt und es werden Anpassungen an den Titeln von bereits existierenden Überwachungstypen vorgenommen.

Absatz 1 Buchstaben a-c bleiben im Wesentlichen unverändert. *Buchstabe d* 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 *Buchstabe e*.

In *Absatz 2 Buchstabe c* heisst es neu *die Bestimmung des Standorts bei der letzten Aktivität* (s. auch die Erläuterungen zu Art. 63).

In *Absatz 3 Buchstabe a* hat sich der Titel der Notsuche wie folgt geändert: *die Bestimmung des Standorts bei der letzten Aktivität* (s. Art. 67 Abs. 1 Bst. a). *Buchstabe b* wird neu eingefügt und verweist auf die beiden neuen Typen der Notsuche zur Posi-

tionsbestimmung (LALS, s. Art. 67 Abs. 1 Bst. b und c). *Buchstaben c, d und e* bleiben unverändert und entsprechen den bisherigen Buchstaben b, c und d. Nur die Verweise zu den entsprechenden Bestimmungen in Klammern sind angepasst.

In *Absatz 4 Buchstabe a* heisst es neu *die Bestimmung des Standorts bei der letzten Aktivität* (s. auch die Erläuterungen zu Art. 63). *Buchstabe b* 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). *Buchstaben c, d und e* bleiben unverändert und entsprechen den bisherigen Buchstaben b, c und d. Nur die Verweise zu den entsprechenden Bestimmungen in Klammern sind angepasst. In *Buchstabe f* wird der Verweis auf den bereits existierenden Antennensuchlauf im Rahmen einer Fahndung (Art. 68 Abs. 1 Bst. g, bisher Bst. d) nachgetragen.

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), sog. 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, i, j und k sowie Abs. 3

In *Absatz 1 Buchstabe b Ziffer 1* werden die Verweise auf die bisher in Artikel 20 geregelten Angaben angepasst. Neu sind in Artikel 20 die Überprüfung der Teilnehmerangaben bei Mobilfunkdiensten, in Artikel 20a die entsprechende Erbringung des Identitätsnachweises bei natürlichen Personen und in Artikel 20b die entsprechende Erbringung des Identitätsnachweises bei juristischen Personen geregelt. In *Ziffer 2* wird bei den «weiteren Kontaktdaten» der jeweilige Gültigkeitszeitraum hinzugefügt. Mit Gültigkeitszeitraum ist die Zeitspanne (Datum des Beginns und gegebenenfalls des Endes) gemeint, von wann bis wann die jeweiligen «weiteren Kontaktdaten» bei der MWP gemeldet sind beziehungsweise waren. Als «weitere Kontaktdaten» kann die MWP beispielsweise weitere ihr bekannte Adressen, Telefonnummern und E-Mail-Adressen des Teilnehmenden mitteilen. Die MWP gibt die bei ihr vorhandenen Daten bekannt. Sie hat keine Pflicht

zur lückenlosen Erfassung und Nachführung der aktuellen Kontaktdaten ihrer Kunden.

In *Absatz 1 Buchstabe c* werden sinngemäss die gleichen Änderungen vorgenommen, wie in Buchstabe b. 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 *Absatzes 1 Buchstabe d* wird eine redaktionelle Änderung im Sinne der geschlechtergerechten Sprache vorgenommen (von der oder dem Teilnehmenden).

In *Absatz 1 Buchstabe d Ziffer 2* erfolgen zwei Änderungen. Erstens wird der bisherige Begriff *Dienstidentifikator* durch *Haupt-Dienstidentifikator* ersetzt, da es Mobilfunkabonnemente mit 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: ein Master (Hauptnummer) und weitere Slaves (Nebennummern). Diese Hierarchie kann in einigen Angeboten von dem oder der Teilnehmenden selbst geändert werden, das heisst er oder sie kann selbst bestimmen, welche SIM-Karte gerade die Hauptnummer benutzt. Dadurch sind einer IMSI mehrere MSISDN zugeordnet. Im einfachen Fall ist einer IMSI nur eine MSISDN zugeordnet. Die Nebennummern sind technische Nummern und dem oder der Teilnehmenden in der Regel nicht bekannt. Falls es nur eine SIM-Karte gibt, ist diese die Hauptnummer und es gibt keine Nebennummern. 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, z. B. wenn der Benutzer nicht das Mobilfunknetz, sondern einen WLAN-Hotspot als Netzzugang benutzt. 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 ersetzt (ICCID ist im Anhang definiert), 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 teilt dem Netz seinen *SUPI* ausschliesslich in verschlüsselter Form mit (z. B. bei der Anmeldung im Netz). 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 oder Dienstidentifikatoren 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. Neu ist der jeweilige Gültigkeitszeitraum des Adressierungselements respektive Identifikators anzugeben.

Um den auskunftsersuchenden Behörden die Auswertung der gelieferten Antworten zu erleichtern und zum besseren Verständnis, um was für einen Dienst es sich handelt, wird in *Ziffer 13* ein Feld für die Übermittlung der Bezeichnung des angefragten Netzzugangsdienstes eingefügt. Das kann bspw. die Verkaufsbezeichnung des Abonnements sein. 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 internationalen Legal Entity Identifier (LEI) gestellt werden (s. Erläuterungen zu Art. 20*b* Abs. 1 Bst. b). In *Buchstabe i* wird *DSL-Identifikator* durch *GPSI* ersetzt (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).

Absatz 3 erster Satz 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

Im Einleitungssatz von *Absatz 1* wird präzisiert, dass diejenigen Angaben zu liefern sind, die im Anfragezeitraum gültig waren respektive sind. Der Anfragezeitpunkt kann von der Gegenwart in die Vergangenheit reichen, aber nicht in die Zukunft. Da es sich bei den Angaben dieses Auskunftstyps um nutzungsabhängige Daten handelt, müssen die auskunftspflichtigen MWP nur die Daten der letzten 6 Monate aufbewahren. Bei länger als 6 Monate in die Vergangenheit reichenden Anfragen, müssen die MWP nur die bei ihnen allfällig noch vorhandenen Daten liefern.

Der zweite Satz des bisherigen *Absatzes 1* wird aus redaktionellen Gründen als neuer *Absatz 2* aufgeführt.

Absatz 1 Buchstabe a bleibt unverändert.

In den *Buchstaben b und c* werden die Identifikatoren aufgrund der Multi-SIM- und Multi-Device-Angebote (s. Art. 35 Abs. 1 Bst. d Ziff. 2) in die Mehrzahl gesetzt und es wird präzisiert, dass es sich um Identifikatoren handelt, die zum angefragten Netzzugangsdienst dazugehören.

In *Buchstabe c* werden neue Identifikatoren des 5G-Systems hinzugefügt: SUPI und GPSI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10 «SUPI» und Art. 35 Abs. 1 Bst. d Ziff. 2 «GPSI»).

In *Buchstabe d* wird ein neuer Identifikator des 5G-Systems hinzugefügt: *PEI*. Der *Permanent Equipment Identifier* (*PEI*) dient zur weltweit eindeutigen Identifikation von Endgeräten in 5G-Mobilfunknetzen. Der *PEI* besteht entweder aus einer *IMEI* oder einer *IMEISV*. Ausserdem wird präzisiert, dass diese Angaben nur für die letzten 6 Monaten erhältlich sind, da es sich um nutzungsabhängige Daten (usage) handelt.

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

In *Buchstabe f* wird die Mitteilung der PUK-Codes (PUK und PUK2) um die Angabe des jeweiligen Gültigkeitszeitraums (s. sinngemäss Art. 35 Abs. 1 Bst. b Ziff. 2) erweitert. Die Angabe des jeweiligen Gültigkeitszeitraums dient der Differenzierung, falls mehrere PUK-Codes mitgeteilt werden. Es sind jeweils die zur angefragten SIM zugehörigen PUK-Codes zu liefern.

Der zweite Satz des bisherigen Absatzes 1 wird aus redaktionellen Gründen neu als separater *Absatz 2* aufgeführt. Der Inhalt bleibt unverändert. Der bisherige Absatz 2 wird neu zu *Absatz 3*.

In *Absatz 3 Buchstabe a* wird in den Beispielen der weniger typische DSL-Identifikator durch GPSI ersetzt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2).

In den *Buchstaben b* und *c* werden die neue Identifikatoren des 5G-Systems SUPI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10) und PEI (s. Art. 36 Abs. 1 Bst. d) eingefügt.

Buchstabe d bleibt unverändert.

Buchstabe e wird neu hinzugefügt, um insbesondere die Abfrage des PUK-Codes 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 abzufragen.

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 kann die Bestimmung hier nun ergänzt werden.

Art. 37 Abs. 1 Einleitungssatz und Bst. b

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

Die Eindeutigkeit des Dienstidentifikators (z. B. Benutzername, Username) in *Buchstabe b* bezieht sich auf die Anbieterin. Dieser Dienstidentifikator dient den berechtigten Behörden bei Bedarf als Suchkriterium für weitere Auskunftsgesuche. Nach Möglichkeit ist der Dienstidentifikator mit einer geeigneten Bezeichnung zu versehen, wenn dessen Bedeutung nicht selbsterklärend ist.

In den Beispielen in *Buchstabe b* wird der DSL-Identifikator durch einen Identifikator des 5G-Systems (GPSI) ersetzt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2).

Art. 38 Auskunftstyp IR_8_IP (NAT): Identifikation der Benutzerschaft bei nicht eindeutig zugeteilten IP-Adressen (NAT)

In der Praxis hat sich gezeigt, dass die Auskunftsgesuche zur Teilnehmeridentifikation anhand der IP-Adresse und weiterer Kriterien im Falle von sogenanntem Carrier-grade NAT (cgNAT) nicht immer zu eindeutigen Ergebnissen führen. Dies liegt da-

ran, dass bei cgNAT die Network Address Translation (NAT) durch die Internetzugangsanbieterin (Carrier) für alle oder einen grossen Teil ihrer Kunden eingesetzt wird und dadurch mehrere Kunden gleichzeitig mit der gleichen öffentlichen Quell-IP-Adresse und möglicherweise auch der gleichen öffentlichen Quell-Portnummer im Internet auftreten können (Pflichtkriterien der Anfrage). Wie auch bei den anderen Auskunftstypen muss es daher möglich sein, mehrere Ergebnisse zuzulassen. Die Möglichkeit von mehrdeutigen Abfrageergebnissen bei NAT wurde bereits im Erläuternden Bericht zur bisherigen VÜPF (S. 43 oben) erläutert.

Um diesem Umstand Rechnung zu tragen, werden in *Absatz 1* sowie in dessen *Buchstaben a* und *b* redaktionelle Anpassungen vorgenommen und Teilnehmender, Teilnehmeridentifikator, Dienstidentifikator sowie Netzzugangsdienst in den Plural gesetzt. Ausserdem wird in *Absatz 1* eine redaktionelle Änderung im Sinne der geschlechtergerechten Sprache vorgenommen.

In *Buchstabe b* wird in den Beispielen der weniger gebräuchliche DSL-Identifikator durch GPSI ersetzt (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2).

Mit den Änderungen in *Absatz 2 Buchstabe f* wird der Zeitpunkt (neu: massgeblicher Zeitpunkt) neu definiert. Gemäss dem Urteil des Bundesverwaltungsgerichts A-6807/2019 hat eine FDA die Randdaten über die Zuteilung und Übersetzung von IP-Adressen und Portnummern (vgl. Art. 21 Abs. 6 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 Art. 38 Abs. 1 VÜPF zu liefern, sofern ihr die ersuchende Behörde die Angaben gemäss Art. 38 Abs. 2 VÜPF für den gesuchten Zeitpunkt bekannt gibt (Ziff. 4.5.1 S. 24). Mit dieser Ergänzung 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.

Art. 39 Auskunftstyp IR_9_NAT: Auskünfte über NAT-Übersetzungskontexte

In diesem Artikel werden die analogen Änderungen wie in Artikel 38 (s. oben) vorgenommen. Ausserdem werden die beiden Abfragemöglichkeiten besser beschrieben:

a) wenn die NAT-Operation mit dem Quell-Adressierungselement (originating IP address) stattgefunden hat,

b) wenn die NAT-Operation mit dem Ziel-Adressierungselement (destination IP address) stattgefunden hat.

Das Quell-Adressierungselement (originating IP address) muss immer in der Anfrage geliefert werden.

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 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 und Identifikatoren 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. Temporär in Abhängigkeit der Benutzung (usage data) zugeordnete Adressierungselemente und Identifikatoren werden nicht hier, sondern mittels des neuen Auskunftsgesuches nach Artikel 48*b* abgefragt. Neu ist der jeweilige Gültigkeitszeitraum des 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 internationalen Legal Entity Identifier (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

In *Absatz 1* wird ergänzt, dass sich die Anfragen auf einen bestimmten Anfragezeitraum beziehen. Entsprechend gelten die Antworten nur für den angefragten Zeitraum. Es sei daran erinnert, dass nur überwachungspflichtige MWP die Randdaten für die letzten 6 Monate aufbewahren müssen (Pflicht zur Randdatenaufbewahrung). Weiter zurückliegenden Angaben können nur geliefert werden, sofern sie noch bei der MWP vorhanden sind. MWP ohne Überwachungspflichten liefern die ihnen vorliegenden Angaben, da sie keine Pflicht zur Randdatenaufbewahrung haben.

Absatz 1 Buchstabe a bleibt unverändert.

In *Buchstabe b* wird der Zusatz «zugehörigen» eingefügt, um zum Ausdruck zu bringen, dass es sich auch um die zum angefragten Dienst zugehörigen (associated) Adressierungselemente 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.

In *Buchstabe c* werden neue Identifikatoren des 5G-Systems eingefügt: SUPI und GPSI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10 «SUPI» und Art. 35 Abs. 1 Bst. d Ziff. 2 «GPSI»). Ausserdem wird jeweils der Zusatz «zugehörigen» eingefügt, um zum Ausdruck zu bringen, dass es sich um mehrere IMSI oder SUPI handeln kann und dass die dazugehörigen MSISDN beziehungsweise GPSI zu liefern sind (Bsp. Mobilfunkdienste mit Extra-SIM-Karten).

In *Buchstabe d* wird ein neuer Identifikator des 5G-Systems eingefügt: *PEI* (s. Art. 36 Abs. 1 Bst. d). Ausserdem wird präzisiert, dass diese Angaben nur für die letzten 6 Monaten erhältlich sind, da es sich um nutzungsabhängige Daten (usage) handelt.

In *Buchstabe e* 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 *Buchstabe f* wird die Mitteilung der PUK und PUK2-Codes um die Angabe des jeweiligen Gültigkeitszeitraums erweitert (s. Erläuterungen zur analogen Änderung in Art. 36 Abs. 1 Bst. f).

Absatz 2 entspricht dem zweiten Satz des bisherigen Absatzes 1 und wird aus redaktionellen Gründen an diesen Platz verschoben.

In *Absatz 3 Buchstabe a* werden die Beispiele gekürzt, d. h. 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. d).

Buchstaben d und *e* bleiben unverändert.

In *Buchstaben f und g* werden die SIM-Nummer (ICCID) und der Code zum Aufladen des Guthabens oder zur Bezahlung der Dienstleistung als Anfragekriterien hinzugefügt (s. Erläuterungen zu den analogen Änderungen in Art. 36 Abs. 2 Bst. e und f).

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 internationalen Legal Entity Identifier (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. 42a **Auskunftstyp IR_51_EMAIL_LAST: Auskünfte über E-Mail-Dienste**

Dieser Auskunftstyp wird neu geschaffen, um die Angaben über die letzte *zugriffsrelevante Aktivität eines E-Mail-Dienstes* (Definition siehe Anhang der VÜPF, Nr. 39) abzufragen. Dies dient zum einen der Identifizierung des Dienstbenutzers. Zum anderen ist der Zeitpunkt des letzten Zugriffs auf den E-Mail-Dienst massgeblich für den sogenannten Abschluss des Kommunikationsvorgangs. Es gilt nämlich für alle in der Mailbox bereits eingetroffenen und gespeicherten Nachrichten, dass deren Kommunikationsvorgang abgeschlossen ist. Für die in der Mailbox gespeicherten Nachrichten, deren Kommunikationsvorgang abgeschlossen ist, kann die Staatsanwaltschaft die Herausgabe nach Artikel 265 StPO verfügen (Edition). Nachrichten, die nach dem letzten Zugriff eingehen, können von den berechtigten Behörden nur im Rahmen einer Echtzeitüberwachung nach Artikel 58 (RT_26_EMAIL_IRI) oder Artikel 59 (RT_27_EMAIL_CC_IRI) erhoben werden.

In der Anfrage kann kein massgeblicher Zeitpunkt angegeben werden. Die MWP müssen bei dem vorliegenden Auskunftstyp nur über die letzte zugriffsrelevante Aktivität Auskunft erteilen und dies nur maximal 6 Monate rückwirkend. Über frühere Aktivitäten, die vor der letzten zugriffsrelevanten Aktivität stattgefunden haben, müssen sie keine Auskunft erteilen. Im Rahmen dieser Auskunft ist keine rückwirkende Erhebung der Zugriffsaktivitäten des E-Mail-Dienstes (History) erhältlich. Die History und die historischen Randdaten können nur über eine rückwirkende Überwachung HD_30_EMAIL (Art. 62) erhoben werden (s. Erläuterungen zu Art. 62).

In *Absatz 1* sind die zu liefernden Angaben geregelt. Gemäss *Buchstabe a* ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der "eindeutige Dienstidentifikator" gemäss *Buchstabe b* bezeichnet den E-Mail-Dienst (Mailbox), auf den sich die Antwort bezieht, eindeutig. In *Buchstabe c* werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt.

In *Absatz 2* wird geregelt, was die Auskunftsanfrage enthalten muss. Beispielhaft sind als Anfragekriterium die E-Mail-Adresse und der Benutzername aufgeführt. Dieses Anfragekriterium muss hinreichend präzise sein, damit die Anbieterin den angefragten E-Mail-Dienst (Mailbox) ermitteln kann.

Art. 43 Abs. 1 Bst. c Einleitungssatz 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 internationalen Legal Entity Identifier (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 ein bestimmtes Push-Token betreffen, das hier anzugeben ist. Das Push-Token ist ein eindeutiger applikations- und gerätespezifischer Identifikator, der für Benachrichtigungen einer App benutzt wird. Mit diesem Push-Token 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 entspricht dem dritten und vierten Satz des bisherigen Absatzes 2.

Art. 43a Auskunftstyp IR_52_COM_LAST: Auskünfte über andere Fernmelde- oder abgeleitete Kommunikationsdienste

Dieser Auskunftstyp wird neu geschaffen, um die Angaben über die letzte *zugriffsrelevante Aktivität eines anderen Fernmelde- oder abgeleiteten Kommunikationsdienstes* (Definition siehe Anhang der VÜPF, Nr. 41) abzufragen. Dies dient zum einen der Identifizierung des Dienstbenutzers. Zum anderen ist der Zeitpunkt des letzten Zugriffs auf den Dienst massgeblich für den sogenannten Abschluss des Kommunikationsvorgangs. In Analogie zu E-Mail gilt nämlich zum Zeitpunkt des letzten Zugriffs auf den Dienst für alle bereits vorher eingetroffenen und gespeicherten Nachrichten, dass deren Kommunikationsvorgang abgeschlossen ist.

Für die im betreffenden Dienst gespeicherten Nachrichten, deren Kommunikationsvorgang abgeschlossen ist, kann die Staatsanwaltschaft die Herausgabe nach Artikel 265 StPO verfügen (Edition).

In der Anfrage kann kein massgeblicher Zeitpunkt angegeben werden. Die MWP müssen bei dem vorliegenden Auskunftstyp nur über die letzte zugriffsrelevante Aktivität Auskunft erteilen und dies nur maximal 6 Monate rückwirkend. Über frühere Aktivitäten, die vor der letzten zugriffsrelevanten Aktivität stattgefunden haben, müssen sie keine Auskunft erteilen. Im Rahmen dieser Auskunft ist keine rückwirkende Erhebung der Zugriffsaktivitäten des Dienstes (History) erhältlich.

In *Absatz 1* sind die zu liefernden Angaben geregelt. Gemäss *Buchstabe a* ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin der oder dem Teilnehmenden einen solchen zugeteilt hat. Der "eindeutige Dienstidentifikator" gemäss *Buchstabe b* bezeichnet den Fernmelde- oder abgeleiteten Kommunikationsdienst, auf den sich die Antwort bezieht, eindeutig im Bereich der Anbieterin. In *Buchstabe c* werden die zu liefernden Angaben über den Ursprung der Verbindung bei der letzten zugriffsrelevanten Aktivität aufgezählt.

In *Absatz 2* wird geregelt, was die Auskunftsanfrage enthalten muss. Beispielhaft sind als Anfragekriterium Nutzeradresse, Pseudonym und Push-Token (s. Erläuterungen zu Art. 43 Abs. 2 Bst. i) aufgeführt. Dieses Anfragekriterium muss hinreichend präzise sein, damit die Anbieterin den angefragten Fernmelde- oder abgeleiteten Kommunikationsdienst ermitteln kann.

Art. 44 Abs. 1 Bst. c und f sowie Abs. 3 Bst. c und d

Die Änderungen in diesem Artikel betreffen lediglich die geschlechtergerechte Sprache. Inhaltlich ändert sich nichts.

Art. 45 Auskunftstyp IR_18_ID: Identitätsnachweis

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.

Art. 46 Abs. 1

Dieser Absatz wird neu geschlechtergerecht formuliert.

Art. 47 Auskunftstyp IR_20_CONTRACT: Vertragskopie

Absatz 1 wird neu 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.

Art. 48 Auskunftstyp IR_21_TECH: Technische Daten

In *Absatz 1* wird präzisiert, dass sich dieses Auskunftsgesuch auf die «am angefragten Standort» vorhandenen Netzelemente bezieht.

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[25] (5G) ein. Die drei Beispiele für eine Area Identity (SAI[26], RAI[27] und TAI[28]) 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

25 **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.

26 **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)

27 **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)

28 **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)

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 sollen daher den Behörden eine geeignete Identifikationsmöglichkeit für ihre Hotspots zur Verfügung stellen, z.B. 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, d. h. den Hotspot vor Ort nicht unverwechselbar bezeichnet, können andere ausreichend genaue Bezeichnungen verwendet werden, z. B. eine kurze Standortbezeichnung. Diese Änderung bedeutet jedoch nicht, dass die BSSID 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, d. h. dass sich die Anfrage auf alle an diesem Standort befindlichen 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_53_ASSOC_PERM: Auskünfte über längerfristig zugeordnete Identifikatoren

Bei der Erbringung von Fernmeldediensten des IP Multimedia Subsystems (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_54_ASSOC_TEMP: sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren

Bei der Erbringung von 5G-Mobilfunkdiensten können 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 in Echtzeit abfragen zu können.

Die Details werden im Annex 1 der VD-ÜPF geregelt. Beispiel: SUPI zu SUCI und umgekehrt.

Die wichtigsten Anwendungsfälle sind:

Für 5G: Eine berechtigte Behörde erfasst mit ihren funktechnischen Geräten (z. B. False Base Station) einen temporären Identifikator (z. B. 5G-S-TMSI/5G-GUTI oder einen verschlüsselten SUCI. Daraufhin macht sie eine Abfrage gemäss diesem neuen Auskunftstyp, um sofort den zugehörigen permanenten Identifikator zu bekommen, d. h. eine SUPI.

Die Antwortzeit dieses neuen Auskunftstyps muss sehr kurz sein (im Bereich von wenigen Sekunden), da sich die temporären Identifikatoren oft ändern (bspw. mindestens bei jedem Service Request oder Paging Occasion oder noch öfter). Diese Auskunft muss daher automatisiert über eine neue Abfrageschnittstelle des Typs LI_HIQR abgefragt und erteilt werden. In der Abfrage (Auskunftsgesuch) darf nur ein einzelner Identifikator (Abs. 2 Bst. a) stehen. 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.

Die Standortangabe (Abs. 2 Bst. b) ist nötig, da der temporäre Identifikator nur lokal eindeutig ist. An einem anderen Standort kann der gleiche temporäre Identifikator zum gleichen Zeitpunkt einem anderen permanenten Identifikator zugeordnet sein.

Beispiele für Abfragen: SUCI, 5G-S-TMSI oder 5G-GUTI.

Art. 48c Auskunftstyp IR_55_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 jedoch gefälscht oder nicht bekannt ist, benötigen die berechtigten Behörden ein Mittel, um den Anruf oder die Mitteilung zurückverfolgen zu können.

Die Anbieterin muss 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, liefern. Sie muss insbesondere keine Angaben über allfällige weitere, vor- oder nachgelagerte Netze einer Verbindung liefern. Beispiel: Ein Anruf fand 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»).

Mit diesem Auskunftstyp wird für FDA mit vollen Pflichten (d.h. FDA, die nicht vom Dienst ÜPF als FDA mit reduzierten Überwachungspflichten erklärt wurden) und für AAKD mit weitergehenden Überwachungspflichten (Art. 52) eine Aufbewahrungspflicht von 6 Monaten für die entsprechenden Randdaten geschaffen (s. auch Art. 21 Abs. 6 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 Gebühr und die Entschädigung sind im Anhang der GebV-ÜPF festgelegt. Die Bearbeitungszeiten sind im Artikel 14 VD-ÜPF geregelt.

Art. 50 Abs. 5-10

Absätze 5 bleibt materiell unverändert.

Absatz 6: 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 Haupt-Targetidentifikator gehören, z. B. bei einer Hauptnummer alle Nebennummern. Dies gilt für alle Arten von Überwachungen (Echtzeit, rückwirkend, Positionsbestimmung, Notsuche, Fahndung). Ausgenommen sind Neben-Targetidentifikatoren (Bsp.: technische Nummern), die nur zu einem bestimmten Endgerät beziehungsweise einer bestimmten SIM gehören. 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 LIID 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.

Wenn bei einer bereits aktiven Echtzeitüberwachung oder periodischen Positionsbestimmung ein neues Endgerät, eine neue SIM oder Nummer zum überwachten Dienst hinzukommt, ist dieses beziehungsweise diese ebenfalls zu überwachen. Es wird dafür keine zusätzliche Gebühr fällig und keine zusätzliche Entschädigung ausgerichtet. Bei Bedarf kann die Anbieterin dafür eine zusätzliche LIID beim Dienst ÜPF anfordern.

In *Absatz 7* wird die Pflicht der FDA näher umschrieben, die von ihnen oder für sie angebrachten Verschlüsselungen zu entfernen (Art. 26 Abs. 2 Bst. c BÜPF). Mit der Formulierung «für sie angebrachte Verschlüsselungen» ist gemeint, dass es um Verschlüsselungen geht, die mit dem öffentlichen Schlüssel der Anbieterin vorgenommen

werden. Auch wenn die Anbieterin diese Verschlüsselung streng genommen nicht selbst angebracht hat, kann sie sie doch entfernen, da sie über den passenden privaten Schlüssel verfügt. Ausserdem wird klargestellt, dass eine Hochstufung zur AAKD mit weitergehenden Auskunfts- oder Überwachungspflichten gemäss Artikel 22 beziehungsweise Artikel 52 auch die Pflicht zur Entfernung der von der Anbieterin oder für sie angebrachten Verschlüsselungen beinhaltet. Damit hat die betreffende AAKD die gleichen Pflichten wie eine FDA. Die in Artikel 26 Absatz 2 Buchstabe c BÜPF genannte Pflicht, die von ihnen angebrachten Verschlüsselungen zu entfernern, gilt somit auch für die AAKD mit weitergehenden Auskunftspflichten.

Bei asymmetrischen Verschlüsselungsverfahren (Verschlüsselung mit öffentlichem Schlüssel des Empfängers und Entschlüsselung mit privatem Schlüssel des Empfängers) ist die Entfernung einer selbst angebrachten Verschlüsselung für die Anbieterin in der Regel nicht mehr möglich. Nur diejenigen Empfänger können die verschlüsselten Daten entschlüsseln, mit deren öffentlichen Schlüssel sie verschlüsselt wurden. Ein allenfalls zusätzlich angebrachter öffentlicher Schlüssel der Anbieterin darf aber die Tatsache der Überwachung nicht offenlegen.

Wenn die Anbieterin also ein asymmetrisches Verschlüsselungsverfahren beim Senden einsetzt, muss sie allenfalls die zu überwachenden Daten erfassen und übermitteln, bevor sie die Verschlüsselung anbringt.

Umgekehrt muss die Anbieterin beim Empfangen von mit ihrem öffentlichen Schlüssel asymmetrisch verschlüsselten Daten die zu überwachenden Daten erfassen und zunächst mit ihrem privaten Schlüssel entschlüsseln, bevor sie sie an den Dienst ÜPF oder die Behörde übermittelt.

Unter geeigneten Punkten sind alle Punkte zu verstehen, wo die Anbieterin die faktische oder rechtliche Kontrolle über die Kommunikation oder die Datenspeicherung hat und wo die zu überwachenden Daten unverschlüsselt erfasst werden können oder wo die Anbieterin die Verschlüsselung entfernen kann.

In *Absatz 8* werden die Pflichten bei der Echtzeitüberwachung von Mobilfunkdiensten um die Überwachung der technischen Teilnehmerdatenbanken wie HLR[29], HSS[30] und UDM[31] 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 9 sieht vor, dass im IP Multimedia Subsystem (IMS) die netzwerkseitige Bestimmung (network provided) der Standortangaben des Targets während der Echtzeitüberwachung gegebenenfalls angestossen werden muss.

29 **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.

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

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

In *Absatz 10* wird geregelt, dass Änderungen der Endgeräte und SIM, die zum überwachten Abonnement beziehungsweise Prepaid dazugehören, durch die MWP zu beobachten sind und sie die Überwachung selbständig an die Veränderungen anzupassen haben. 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 anfordern.

Art. 53 Abs. 1

In dieser Bestimmung 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.

Art. 54 **Überwachungstyp RT_22_NA_IRI: Echtzeitüberwachung von Randdaten bei Netzzugangsdiensten**

Absatz 1 bleibt unverändert.

Mit 5G sind neu Mehrfacheinbuchungen (multiple registrations) respektive Mehrfachanbindungen (multiple attachments) im gleichen oder in verschiedenen diensterbringenden Netzwerken möglich, was auch einen Wechsel des Ziels der Überwachung (Target) zwischen den verschiedenen Netzwerken und Technologien ermöglicht[32].

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 und *d* bleiben unverändert.

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. d «PEI»).

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 unter anderem die Änderung der Dienstunterstützung (service support), zum Beispiel

32 Vgl. dazu 3GPP TS 33.501 Abschnitt 6.3.2.

Änderungen des PDP Context, des Bearer oder der PDU Session, und die Aktualisierung der Position des Targets, zum Beispiel Location Update und Mobility Registration Update. 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 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. 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 *Altersangabe* ist die Zeitspanne zu verstehen, die zwischen der tatsächlichen Bestimmung der Standortangabe und der Übermittlung dieser Information vergangen ist.

Im neuen *Buchstaben i* wird die Lieferung wichtiger Randdaten geregelt, die bei der Überwachung von technischen Teilnehmerdatenbanken wie HLR, HSS und UDM (s. Erläuterungen zu Art. 50 Abs. 8) erfasst werden können. Es handelt sich um:

- Informationen über das vorherige und das aktuelle diensterbringende Netz, d. h. Ereignisse vom Typ «Serving System» (*diensterbringendes Netz*, z. B. Serving PLMN, VPLMN ID);
- Informationen über die Änderung der zugeordneten Dienst- und Geräteidentifikatoren (z. B. IMSI, MSISDN, IMEI, SIP-URI, IMPI), d. h. Ereignisse vom Typ Susbcriber Record Change;
- 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 *Absatz 3* wird eine redaktionelle Änderung vorgenommen, indem der bisher in jedem einzelnen Buchstaben des Absatzes 3 enthaltene «Typ der benutzten Mobilfunktechnologie» hier einmalig geregelt wird.

In *Buchstabe a* werden, analog zu Artikel 48 Absatz 2 Buchstabe a (s. dortige Erläuterungen), zwei Änderungen vorgenommen: statt beispielhaft die einzelnen Identifikatoren aufzuzählen, wird der allgemeine Begriff der Zell- oder Gebietsidentifikatoren verwendet und es wird «eine andere geeignete Bezeichnung (z. B. Hotspotname)»

als Alternative zur BSSID hinzugefügt. Es genügt hier eine ausreichend genaue Bezeichnung des WLAN-Zugangs, d. h. die gelieferte Bezeichnung muss den WLAN-Zugang am Ort zweifelsfrei identifizieren (s. auch die Erläuterungen zu Art. 48 Abs. 3 Bst. b). Der Hotspotname ist im Parameter *SSID* zu übermitteln.

Buchstaben b und *c* bleiben inhaltlich unverändert. Nur das Wort WLAN-Zugangspunkt wird durch WLAN-Zugang in Buchstabe c ersetzt (s. oben Ersatz von Ausdrücken, Abs. 1).

Die Ergänzungen in den *Buchstaben d* und *e* betreffen die Standortangaben bei einem nichtvertrauenswürdigen, englisch «untrusted» (*Bst. d*) und einem vertrauenswürdigen, englisch «trusted» (*Bst. e*) Nicht-3GPP-Zugang zum Mobilfunkkernnetz. Mit «nichtvertrauenswürdig» und «vertrauenswürdig» wird die Art des Zugangs aus Sicht der Mobilfunkanbieterin unterschieden.

Den mit «nichtvertrauenswürdig» gekennzeichneten Zugängen vertraut die Mobilfunkanbieterin nicht. Es handelt sich meist um Fremdzugänge, d. h. von anderen Anbieterinnen betriebene Zugänge, bei denen die Mobilfunkanbieterin lediglich die IP-Verbindungsdaten kennt (s. dazu auch die Erläuterungen im Anhang «Begriffe und Abkürzungen»). Zwischen dem Endgerät des Targets und dem Gateway (evolved Packet Data Gateway) der Mobilfunkanbieterin wird eine gesicherte (verschlüsselte) Verbindung (VPN) aufgebaut. Die Mobilfunkanbieterin teilt die für sie sichtbare öffentliche Quell-IP-Adresse und gegebenenfalls die Quell-Portnummer des Endgeräts des Targets mit.

Der Zusatz «vertrauenswürdig» bedeutet, dass die Anbieterin diesem Zugang vertraut, da er meist von ihr selbst betrieben wird. Ein solcher Zugang wird auch als Trusted WLAN Access Network (TWAN) bezeichnet. Falls die Postadresse des Zugangs zusätzlich zur Bezeichnung des Netzzugangs (TWAN Identifikator) bekannt ist, ist diese ebenfalls mitzuteilen.

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

Absatz 1 wird vereinfacht und besteht nur noch aus dem ersten Satz des früheren Absatzes 1. Dieser definiert die vom Überwachungstyp RT_24_TEL_IRI betroffenen Dienste.

Der neue *Absatz 2* besteht aus dem zweiten Satz des bisherigen Absatzes 1 und spezifiziert die Randdaten, welche in Echtzeit zu übermitteln sind. *Buchstabe a* entspricht dem bisherigen Absatz 1 Buchstabe a. In *Buchstabe b* wird ein neuer Identifikator des 5G-Systems eingefügt: SUPI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 10). *Buchstaben c* und *d* entsprechen den bisherigen Buchstaben c und d von Absatz 1 mit einer redaktionellen Anpassung wegen der geschlechtergerechten Sprache in Buchstabe c.

Buchstabe e Ziffern 1, *3*, *5*, *6*, *7* und *8* entsprechen den Ziffern des bisherigen Buchstabens e des Absatzes 1. In *Ziffern 2* und *4* werden neue Identifikatoren des 5G-Systems eingefügt: GPSI und PEI (s. Erläuterungen zu Art. 35 Abs. 1 Bst. d Ziff. 2 «GPSI» und Art. 36 Abs. 1 Bst. d «PEI»). In *Ziffer 9* wird präzisiert, dass diese Be-

stimmung nur für Mobilfunk und WLAN anwendbar ist. Es wird ausserdem neu aufgenommen, dass die aktuellen Standortangaben soweit wie möglich vom Netzwerk zu bestimmen und dementsprechend zu kennzeichnen sind (s. Erläuterungen zu Art. 54 Abs. 2 Bst. h). Bei EPS und 5GS sind die Standortangaben, soweit verfügbar, mit dem jeweiligen verknüpften Zeitstempel und jeweils mit dem Alter der Standortangabe (s. Erläuterungen zu Art. 54 Abs. 2 Bst. h) zu ergänzen. Ausserdem wird der Begriff WLAN-Zugangspunkt durch WLAN-Zugang ersetzt (s. Erläuterungen zum Ersatz von Ausdrücken, Abs. 1)

In *Buchstabe f* wird die Lieferung wichtiger Randdaten geregelt, die bei der Überwachung von technischen Teilnehmerdatenbanken wie HLR, HSS und UDM (s. Erläuterungen zu Art. 50 Abs. 8) erfasst werden können (s. Erläuterungen zu Art. 54 Abs. 2 Bst i).

Statt die mit Artikel 54 Absatz 3 identischen Standortangaben an dieser Stelle in einem Absatz 3 noch einmal zu wiederholen, wird in Absatz 2 Buchstabe e Ziffer 9 auf Artikel 54 Absatz 3 verwiesen. Auf diesen 3. Absatz in Artikel 56 kann demzufolge verzichtet werden.

Art. 56a Überwachungstyp RT_56_POS_IMMED: einmalige, sofortige Positionsbestimmung durch das Netzwerk

Standort und *Position* haben in dieser Verordnung eine unterschiedliche Bedeutung. Bisher gab es nur Standortangaben (location information). Unter *Standort* versteht man die Zelle oder das Gebiet, wo sich das Ziel der Überwachung (Target) befindet. Der *Standort* ist in der Regel nur eine grobe Näherung des Ortes, wo sich das Target (Endgerät) tatsächlich befindet und entspricht meist dem Ort, wo sich die Antenne befindet (Antennenstandort), mit der das Target verbunden ist oder zuletzt verbunden war. Die Ungenauigkeit der Standortangabe kann sehr gross sein und hängt von der Reichweite der jeweiligen Antenne ab. Im ländlichen Raum sind bis zu 30 km Abweichung zwischen dem Antennenstandort und der tatsächlichen Position des Targets möglich. Der *Standort* ist dem Mobilfunknetz meist bereits bekannt und muss dann nicht bestimmt werden. Es kann aber auch vorkommen, dass der Standort durch das Mobilnetz bestimmt werden muss, beispielsweise bei einer Notsuche EP_35_PAGING oder bei einer Überwachung HD_31_PAGING.

Unter *Position* versteht man dagegen den präzisen Ort, wo sich das Target (Endgerät) im Moment der Positionsbestimmung tatsächlich befindet. Die Positionsbestimmung ist eine neue Funktion im Mobilfunknetz. Die Positionsbestimmung nach BÜPF (LALS, Lawful Access to Location Services) wird neu eingeführt und gilt als Überwachung nach Artikel 269 StPO. Sie wird nur auf Anordnung der Behörden ausgeführt, die zur Anordnung einer Überwachung berechtigt sind. Die Anordnung muss vom Zwangsmassnahmengericht genehmigt werden. Es werden zwei Überwachungstypen der Positionsbestimmung mittels LALS eingeführt:

1) Einmalige, sofortige Positionsbestimmung (der vorliegenden 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 überwachten Identifikator (Target-ID) assoziierten mobilen Endgeräten zu bestimmen.

Die technischen Ausführungsvorschriften werden vom EJPD in der VD-ÜPF und ihrem Anhang 1 erlassen (*Abs. 2*). Es liegen bisher noch keine praktischen Erfahrungen mit dieser neuen einmaligen Positionsbestimmung mittels LALS 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) und, soweit möglich, der zu diesem Zeitpunkt letzte bekannte Zellstandort dieses Endgeräts mitzuteilen, das heisst der Antennenstandort der diensterbringenden Zelle.

Art. 56*b* Überwachungstyp RT_57_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.

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 überwachten Identifikator (Target-ID) assoziierten mobilen Endgeräten zu bestimmen.

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 Intervallen erfolgt. Da bisher noch keine praktischen Erfahrungen mit dieser neuen periodisch wiederkehrenden Positionsbestimmung mittels LALS vorliegen, insbesondere hinsichtlich des Ressourcenverbrauchs und des Zeitbedarfs der Positionsbestimmung, 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) und, soweit möglich, der zu diesem Zeitpunkt letzte bekannte Zellstandort dieses Endgeräts mitzuteilen, das heisst der Antennenstandort der diensterbringenden Zelle.

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

Die *Buchstaben a-d, f* und *i* bleiben materiell unverändert.

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. d «PEI»).

In *Buchstabe g Ziffer 1* 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 *Ziffern 2* und *3* bleiben unverändert.

In *Buchstabe h* wird aufgrund der Erfahrungen aus der Praxis die Möglichkeit von anderen geeigneten Bezeichnungen wie «Hotspotname» eingefügt, obwohl es sich dabei nicht um eindeutige Identifikatoren handelt. Es genügt hier eine ausreichend genaue Bezeichnung des WLAN-Zugangs, d. h. die gelieferte Bezeichnung muss den WLAN-Zugang am Ort ausreichend genau identifizieren (s. Erläuterungen zu Art. 48 Abs. 2 Bst. a). Der Hotspotname ist im Parameter *SSID* zu übermitteln.

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 den bisherigen Buchstabe i.

Die neuen *Buchstaben k* und *l* regeln die Lieferung von Standortangaben bei sogenannten nichtvertrauenswürdigen und vertrauenswürdigen Nicht-3GPP-Zugängen zum Mobilfunkkernnetz und entsprechen den Änderungen in Artikel 54 Absatz 3 Buchstaben d und e (s. dortige Erläuterungen).

Art. 61 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 zu Art. 36 Abs. 1 Bst. d «PEI»).

Für die Ergänzung im einleitenden Satz zum *Buchstaben g* betreffend «vom Netzwerk bestimmte und dementsprechend gekennzeichnete aktuelle Standortangaben» vergleiche die Erläuterungen zu Artikel 56 Absatz 1 Buchstabe e Ziffer 9. In *Ziffer 1* werden analog zu Artikel 60 Buchstabe g Ziffer 1 «die verknüpften Zeitstempel» hinzugefügt (s. dortige Erläuterungen). Die *Ziffern 2* und *3* bleiben unverändert. Die neue *Ziffer 4* regelt die Lieferung von Standortangaben bei sogenannten nichtvertrauenswürdigen Nicht-3GPP-Zugängen zum Mobilfunkkernnetz und ist vergleichbar mit der Änderung in Artikel 54 Absatz 3 Buchstabe d (s. die dortigen Erläuterungen).

In *Buchstabe g^{bis}* wird, wie in Artikel 60 Buchstaben 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 erster Gedankenstrich* wird eine redaktionelle Änderung vorgenommen, um klarzustellen, dass sich der Verweis zu Buchstabe g auf die Standortangaben bezieht. Beim *zweiten Gedankenstrich* 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). Der Hotspotname ist im Parameter *SSID* zu übermitteln.

Nach *Buchstabe j* sind nun auch die Angaben über das unmittelbar benachbarte Netz «von» und das unmittelbar benachbarte Netz «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 nachverfolgen und damit die entsprechenden Ursprünge der Kommunikation oder des Kommunikationsversuches identifizieren zu können (s. auch Erläuterungen zu Art. 48*c*). Dieser Ansatz 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 1 Buchstabe e verzichtet.

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

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 ermöglicht wird.

Die Speicherpflicht für die Randdaten von E-Mail-Diensten (History) haben übrigens nur MWP mit vollen Überwachungspflichten, d. h. FDA, die nicht nach Artikel 51 befreit sind, und AAKD mit weitergehenden Überwachungspflichten (Art. 52). Alle anderen MWP liefern lediglich die ihnen vorliegenden Daten.

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

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 überwachten Identifikator assoziierten Endgeräten (also gegebenenfalls nicht nur von einem) festzustellen ist.

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 Ziffer 1* die beispielhafte Aufzählung von Identifikatoren verkürzt, ähnlich wie in Artikel 48 Absatz 2 Buchstabe a (s. die dortigen Erläuterungen). Ausserdem werden die «verknüpften Zeitstempel» eingefügt (s. die Erläuterungen zu Art. 54 Abs. 2 Bst. h) und die beteiligten Zellen werden in den Plural gesetzt (ebenso in *Ziff. 3*), da in 4G- und 5G-Netzen ein Endgerät von mehreren Zellen bedient werden kann (Master Node und ein oder mehrere Secondary Nodes).

Letzteres dient zur Erhöhung der Bandbreite, indem die Zellen eine sogenannte «Carriers Aggregation» vornehmen.

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. 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). Der Hotspotname ist im Parameter *SSID* zu übermitteln.

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). Der Hotspotname ist im Parameter *SSID* zu übermitteln.

Art. 67 **Überwachungstypen EP: Notsuche**

Absatz 1 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 überwachten Identifikator (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. auch die Erläuterungen zu Art. 50 Abs. 6). 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_58_POS_IMMED, die einmalige, sofortige Positionsbestimmung durch das Netzwerk von allen mit dem überwachten Identifikator (Target-ID) assoziierten mobilen Endgeräten der vermissten oder einer dritten Person im Rahmen einer Notsuche. Technisch entspricht

dieser Typ dem neuen Überwachungstyp RT_56_POS_IMMED (s. auch die Erläuterungen zu Art. 56*a*).

Ebenfalls neu ist der in *Buchstabe c* definierte Typ EP_59_POS_PERIOD, die periodisch wiederkehrende Positionsbestimmung durch das Netzwerk von allen mit dem überwachten Identifikator (Target-ID) assoziierten mobilen Endgeräten der vermissten oder einer dritten Person im Rahmen einer Notsuche. Technisch entspricht dieser Typ dem neuen Überwachungstyp RT_57_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 Buchtaben 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. Das Vorgehen ist entsprechend wie unter Buchstabe d erläutert. Die Unterschiede zu Buchstabe d bestehen darin, dass es sich um rückwirkende Überwachungen handelt, 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 ihr assoziierten Nummern abgedeckt sind, und dass für die rückwirkenden Überwachungen keine Aufhebungsaufträge erforderlich sind.

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. d «PEI»).

Absatz 2 präzisiert, dass sich der Beginn und das Ende einer rückwirkenden Überwachung gemäss Absatz 1 Buchstabe f nach den Bestimmungen des Artikels 4*a* richten (s. die dortigen Erläuterungen).

Art. 68 Fahndung

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. 74a **Übergangsbestimmung zur Änderung vom xx.xx.xxxx**

Um die Einführung der neuen Auskunfts- und Überwachungstypen zwischen den MWP und dem Dienst ÜPF zu synchronisieren, ist es vorliegend sinnvoll, detaillierte Übergangsbestimmungen für die einzelnen Änderungen vorzusehen. Innerhalb der

vorgesehenen Fristen sind die technischen Anpassungen auf Seiten der genannten MWP 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.

Absatz 1 sieht eine Übergangsfrist für die hier näher bezeichneten MWP von 12 Monaten nach Inkrafttreten dieser Verordnungsrevision betreffend vier neue Auskunftstypen vor:

1. IR_51_EMAIL_LAST (Auskünfte über E-Mail-Dienste; Art. 42*a*),
2. IR_52_COM_LAST (Auskünfte über abgeleitete Kommunikationsdienste; Art. 43*a*)
3. IR_53_ASSOC_PERM (Auskünfte über längerfristig zugeordnete Identifikatoren; Art. 48*a*),
4. IR_55_TEL_ADJ_NET (Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten*, Art. 48*c).

Absatz 2 gibt den MWP mit vollen Pflichten eine längere Übergangsfrist von 24 Monaten nach Inkrafttreten dieser Verordnungsrevision für den fünften neuen Auskunftstyp IR_54_ASSOC_TEMP (sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren; Art. 48*b*), da dieser umfangreichere Anpassungen erfordert (s. auch die Erläuterungen zu Art. 18 Abs. 3). Für die Umsetzung der beiden neuen Typen der einmaligen, sofortigen Positionsbestimmung nach Artikel 56*a* (RT_56_POS_IMMED) und Artikel 67 Absatz 1 Buchstabe b (EP_58_POS_IMMED) wird dagegen eine relativ kurze Übergangsfrist von 12 Monaten nach Inkrafttreten dieser Verordnungsrevision gewährt. Aufgrund des zu erwartenden Zusatznutzens dieser neuen Überwachungstypen sollen sie den Strafverfolgungsbehörden möglichst rasch zur Verfügung stehen.

Absatz 3 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 MWP mit vollen Pflichten die Speicherung der hierfür notwendigen Daten innert zwölf Monaten nach dem Inkrafttreten dieser Verordnungsrevision sicherstellen. Zweitens müssen sie spätestens 18 Monate nach dem Inkrafttreten dieser Verordnungsrevision die neuen rückwirkenden Daten (Art. 61 Bst. j) liefern können.

Absatz 4 regelt die Übergangsbestimmung für die MWP mit vollen Pflichten betreffend die beiden neuen Typen der periodischen Positionsbestimmung nach Artikel 56*b* (RT_57_POS_PERIOD) und Artikel 67 Absatz 1 Buchstabe c (EP_59_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 absehbarer Zeit durch eine Neubeschaffung ersetzt wird. Die Implementierung müsste sonst zwei Mal vorgenommen werden: einmal in die aktuelle Komponente und dann nochmals in die neue Komponente. Die Machbarkeit der Implementierung in die aktuelle Komponente ist zudem 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 genannten MWP erhalten nach der vollständigen Inbetriebnahme der neuen Echtzeitsystemkomponente noch bis zu 18 Monate Zeit für die nötigen Anpassungsarbeiten in ihren Systemen und für die Durchführung der notwendigen Tests mit dem Dienst ÜPF.

Absatz 5 bildet das Gegenstück zu Absatz 1 1. Teil und Absatz 2 und bestimmt die gleiche relativ kurze Übergangsfrist von 12 Monaten nach dem Inkrafttreten dieser Verordnungsrevision für den Dienst ÜPF betreffend die entsprechenden Auskunfts- und Überwachungstypen. Die beiden neuen Typen der einmaligen, sofortigen Positionsbestimmung nach Artikel 56a (RT_56_POS_IMMED) und Artikel 67 Absatz 1 Buchstabe b (EP_58_POS_IMMED) sollen ebenfalls in die neue Echtzeitsystemkomponente des Verarbeitungssystems des Dienstes ÜPF implementiert werden.

Absatz 6 regelt analog zu Absatz 3 die Übergangsfrist von 18 Monaten für den Dienst ÜPF, um für die Entgegennahme der entsprechenden historischen Daten bereit zu sein.

Absatz 7 entspricht dem zweiten Teil von Absatz 1.

Absatz 8 bildet das Gegenstück zu Absatz 4 betreffend den Dienst ÜPF.

5.2 Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF)

Art. 3 Abs. 4 Bst. a und b, 4bis und 5

Absatz 4 Buchstabe a wird mit dem neuen Auskunftstyp IR_53_ASSOC_PERM (Art. 48*a*) ergänzt. In *Buchstabe b* werden vier neue Auskunftstypen IR_51_EMAIL_LAST (Art. 42*a* VÜPF), IR_51_COM_LAST (Art. 43*a* VÜPF), IR_54_ASSOC_TEMP (Art. 48*b* VÜPF) und IR_55_TEL_ADJ_NET (Art. 48*c* VÜPF) hinzugefügt.

Absatz 4bis wird mit dem neuen Auskunftstyp IR_53_ASSOC_PERM (Art. 48*a*) ergänzt.

In *Absatz 5* wird «zeitnah» präzisiert. Neu müssen die Antennensuchläufe innerhalb von 24 Stunden angeordnet werden, damit diese Regelung zur Anwendung kommt. Der Dienst ÜPF erstellt wie bisher eine Berechnung nach den Artikeln 13 und 17 (Gebühren und Entschädigungen für nicht aufgeführte Dienstleistungen).

Art. 15 **Anspruch**

Die *Sachüberschrift* wird von «Entschädigungsanspruch» zu «Anspruch» geändert. Artikel 38 Absatz 2 BÜPF[33] sieht vor, dass die MWP vom Dienst ÜPF eine angemessene Entschädigung[34] für die Kosten erhalten, die ihnen durch die Durchführung der Überwachungen und die Erteilung der Auskünfte nach den Artikeln 21 und 22 entstehen.

Absatz 1 wird materiell nicht geändert. Anspruch auf eine Entschädigung haben die MWP gemäss Artikel 2 Buchstaben a–e BÜPF, das heisst alle MWP ausser die professionellen Wiederverkäuferinnen (Art. 2 Bst. f BÜPF), sofern sie ihre Auskunfts- und Überwachungspflichten gemäss dem BÜPF und der VÜPF erfüllen, dies unabhängig davon, ob sie eine Bestätigung über die Auskunfts- und Überwachungsbereitschaft haben oder nicht (Art. 33 Abs. 6 BÜPF, Art. 31 VÜPF). Die MWP, die ihre Auskunfts- und Überwachungspflichten gemäss dem BÜPF und der VÜPF nicht erfüllen, haben keinen Anspruch auf eine Entschädigung. Die MWP, die ihre Pflichten teilweise erfüllen, indem sie zum Beispiel den Dienst ÜPF unterstützen, können gemäss Artikel 19 Absatz 2 entschädigt werden.

In Absatz 2 wird neu geregelt, dass die MWP eine Entschädigung auch erhalten können, wenn sie bei der Erteilung von Auskünften oder Durchführung von Überwachungen den Dienst ÜPF unterstützen, obwohl sie selber nicht zur Erteilung von Auskünften oder zur Durchführung von Überwachungen verpflichtet sind. Dabei geht es zum Beispiel um Arbeiten wie den Internetzugang zu organisieren, dem Dienst ÜPF den problemlosen Zugang zu den Servern zu gewähren (soweit es Kosten generiert) oder Anpassungen an der Infrastruktur. Im Gegenteil zu Absatz 1 besteht für die betroffenen MWP kein Anspruch auf eine Entschädigung («Kann-Vorschrift»). Es ist möglich, gewisse Kosten der MWP nicht zu entschädigen, wie z.B. den zusätzlich verbrauchten Strom. Hier handelt es sich insbesondere um FDA mit reduzierten Überwachungspflichten (Art. 51 VÜPF), um AAKD ohne weitergehende Auskunfts- und Überwachungspflichten (s. Art. 22 und 52 VÜPF), aber auch um Betreiberinnen von internen Fernmeldenetzen oder um Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen.

Im neuen *Absatz 3* wird die Regelung des bisherigen Artikels 16 übernommen.

Art. 16 Aufgehoben

Die Regelung dieser Bestimmung wird als Absatz 3 in Artikel 15 übernommen. Deshalb wird Artikel 16 aufgehoben.

Art. 17 Abs. 3 und 3bis

Der aktuelle Absatz 4, der die Regelung betreffend der 80 Prozent für die Entschädigung beinhaltet, deckt sich mit dem Schluss des 3. Absatzes. Deshalb kann der Teilsatz «und davon nur 80 Prozent» in *Absatz 3* gestrichen werden.

33 Fassung in Kraft ab 01.01.2022
34 «angemessene Entschädigung»; s. Urteil des Bundesgerichts vom 27.07.2021 (2C_650/2020)

Absatz 3bis regelt die Maximalhöhe der Entschädigung ähnlich wie Artikel 19 Absatz 2 dritter Satz.

Art. 18 Fälle der Kostenübernahme

Aufgrund der formellen Anpassungen in der VÜPF im Zusammenhang mit der Kategorie der AAKD wird auch in diesem Erlass die Bezeichnung «AAKD mit weitergehenden Pflichten gemäss Artikel 22 oder 52 VÜPF» verwendet (vergleiche z. B. Art. 11 Abs. 1 Bst. a und Art. 19 Abs. 1 VÜPF).

Art. 19 Abs. 1

In *Absatz 1* wird auf Artikel 13 (Gebühr für nicht aufgeführte Dienstleistungen) verwiesen. Mit diesem Verweis legt der Dienst ÜPF die Gebühr, für die bei ihm entstandenen Kosten, welche ihm aufgrund der unzureichenden Mitwirkung einer MWP entstanden sind, fest. Dies weil der Dienst ÜPF anstelle einer MWP Mehrarbeit leistet, welche die reine Gebühr übersteigt. Mit dem Wort «nach Zeitaufwand» war der Verweis auf Artikel 13 zu restriktiv, weil in diesem Fall nur Absatz 1 anwendbar ist. Mit der vorliegenden Änderung (Streichung von «nach Zeitaufwand») betrifft der Verweis nun auch Absatz 2 von Artikel 13. Somit kann auch die Bereitstellung von einmalig benutztem Material nun direkt gestützt auf die GebV-ÜPF in Rechnung gestellt werden. Bei einmalig benutztem Material hat der Dienst ÜPF von Fall zu Fall zu entscheiden, ob das Material der MWP nach Beendigung der Überwachungsmassnahme übergeben werden kann oder nicht. Mehrmals benutztes Material wird im Stundenaufwand eingerechnet. Ein Spezialfall bei einer MWP kann nach dieser Verrechnungsmethode hohe Kosten verursachen. Deshalb ist es für die anordnende Behörde empfehlenswert, im Voraus mit dem Dienst ÜPF Rücksprache über die Kostenhöhe zu halten.

Anhang

Der Anhang der Gebührenverordnung besteht aus der Tabelle, welche sämtliche Auskunfts- und Überwachungstypen und in der Gebührenverordnung definierten Gebühren aufzeigt. Es ist sowohl die Gebühr für den Dienst ÜPF, wie auch die Entschädigung pro involvierte MWP ersichtlich. Die Tabelle ermöglicht es sämtlichen anordnenden und auswertenden Behörden, die anfallenden Kosten für eine geplante Überwachungsmassnahme im Voraus zu berechnen. Werden Parameter wie die Anzahl der involvierten MWP benötigt, kann der Dienst ÜPF zu Rate gezogen werden. Grundsätzlich schulden die anordnenden Behörden dem Dienst ÜPF sowohl die «Gebühren Dienst ÜPF», wie auch die «Entschädigungen Mitwirkungspflichtige». Für Auskünfte gemäss den Artikeln 27, 35, 37, 40, 42, 43 und neu 48*a* VÜPF werden seit dem 1. Juli 2020 den anordnenden Behörden keine Gesamtgebühr (bestehend aus «Gebühr Dienst ÜPF» und «Entschädigung Mitwirkungspflichtige») mehr in Rechnung gestellt. Den MWP wird weiterhin die «Entschädigung Mitwirkungspflichtige» in der Höhe von 3 Franken ausgerichtet. Die damit entgehenden Einnahmen des Dienstes ÜPF wurden auf Empfehlung der Arbeitsgruppe «Finanzierung FMÜ» mit

einer Gebührenerhöhung bei den Echtzeit- und den rückwirkenden Überwachungen kompensiert[35].

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

1) der Auskunftstyp IR_51_EMAIL_LAST, Auskünfte über E-Mail-Dienste (Art. 42*a* VÜPF);
2) der Auskunftstyp IR_52_COM_LAST, Auskünfte über andere Fernmelde- oder abgeleitete Kommunikationsdienste (Art. 43*a* VÜPF)
3) der Auskunftstyp IR_53_ASSOC_PERM, Auskünfte über längerfristig zugeordnete Identifikatoren (Art. 48*a* VÜPF);
4) der Auskunftstyp IR_54_ASSOC_TEMP, sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren (Art. 48*b* VÜPF);
5) der Auskunftstyp IR_55_TEL_ADJ_NET, Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten (Art. 48*c* VÜPF);
6) der Überwachungstyp (Echtzeitüberwachung) RT_56_POS_IMMED, einmalige, sofortige Positionsbestimmung durch das Netzwerk (Art. 56*a* VÜPF);
7) der Überwachungstyp (Echtzeitüberwachung) RT_57_POS_PERIOD, periodisch wiederkehrende Positionsbestimmung durch das Netzwerk (Art. 56*b* VÜPF);
8) der Überwachungstyp (Notsuche) EP_58_POS_IMMED, einmalige, sofortige Positionsbestimmung durch das Netzwerk (Art. 67 Abs. 1 Bst. b VÜPF); sowie
9) der Überwachungstyp (Notsuche) EP_59_POS_PERIOD, periodisch wiederkehrende Positionsbestimmung durch das Netzwerk (Art. 67 Abs. 1 Bst. c VÜPF).

Dies erfordert eine entsprechende Teilrevision des Anhangs GebV-ÜPF.

Grundsätzlich werden bei der Festlegung neuer Gebühren und Entschädigungen die neuen Auskunfts- und Überwachungstypen ins Verhältnis zu den bestehenden Auskunfts- und Überwachungstypen gesetzt. Die Gebührenhöhe wird von weiteren Kriterien beeinflusst wie die Unterhalts-, Amortisations- und Investitionskosten für das Verarbeitungssystem. Bei der Festlegung der neuen Gebühren spielt ebenfalls die Häufigkeit der Nutzung der neuen Auskunfts- und Überwachungstypen eine Rolle.

Vorliegend entsprechen die Gebühren und Entschädigungen für die neuen Auskunftstypen den bisherigen Beträgen. Unter den neuen Auskunftstypen kann nur der Auskunftstyp IR_53_ASSOC_PERM (Art. 48*a* VÜPF) als «einfache» Auskunft betrachtet werden. Dementsprechend erhebt der Dienst ÜPF hierfür keine Gebühr, die MWP bekommt jedoch eine Entschädigung von Fr. 3.- pro Ergebnisdatensatz. Die übrigen neuen Auskunftstypen gelten als «komplexe» Auskünfte und es wird pro Auskunftsgesuch eine Gebühr von Fr. 75.- für den Dienst ÜPF und eine Entschädigung von Fr. 125.- für die MWP festgelegt.

Bei den neuen Überwachungstypen bestehen weniger Gemeinsamkeiten mit den bisherigen Typen. Die beiden neuen Überwachungstypen zur Positionsbestimmung durch das Netzwerk (LALS) bieten eine völlig neue Funktionalität. Die Gebühr und Entschädigung für die einmalige, sofortige Positionsbestimmung RT_56_POS_IMMED (Art. 56*a* VÜPF) orientieren sich daher an denen des entfernt

35 S. Teilrevision der GebV-ÜPF vom 20.05.2020, in Kraft seit dem 01.07.2020 (AS **2020** 2061) und erläuternden Bericht.

vergleichbaren Typs HD_31_PAGING (Art. 63 VÜPF) und sind jeweils Fr. 50.- höher angesetzt, da der Aufwand für den Dienst ÜPF und die MWP steigen wird. Dieser neue Überwachungstyp bietet aufgrund der viel genaueren Positionsbestimmung einen wesentlichen Mehrwert im Vergleich zu HD_31_PAGING.

Der zweite neue Überwachungstyp zur Positionsbestimmung durch das Netzwerk (LALS), RT_57_POS_PERIOD (Art. 56*b* VÜPF), entspricht einer typischen Echtzeitüberwachung von der Aktivierung bis zur Deaktivierung. In festen periodischen Abständen bestimmt das Netzwerk die aktuelle genaue Position des Endgeräts der überwachten Person und liefert die Position sofort an das Verarbeitungssystem weiter. Die Gesamtgebühr ist etwas höher als die der Echtzeitüberwachungstypen «nur Randdaten». Sie beträgt ein Mehrfaches der Gesamtgebühr für die einmalige, sofortigen Positionsbestimmung RT_54_POS_IMMED (Fr. 2 800.- gegen Fr. 600.-), weil das Verarbeitungssystem angepasst werden muss, um die Positionsangaben entgegennehmen und verarbeiten zu können.

Da die Notsuche ein zentrales Element zur Lebensrettung sein kann und nur in Fällen genutzt werden darf, bei denen Leib und Leben eines Menschen gefährdet sind, werden hier, wie auch bei den anderen Überwachungstypen der Notsuche, tiefere Gebühren und Entschädigungen festgesetzt als bei vergleichbaren Überwachungen. Ausserdem wird bei der Gebühr auf einen Zuschlag für die Positionsbestimmungen (einmalig oder periodisch) im Rahmen einer Notsuche verzichtet. Somit ist die Gebühr für EP_58_POS_IMMED (Art. 67 Bst. b VÜPF) von Fr. 50.- die gleiche wie die Gebühren für die anderen Überwachungstypen der Notsuche. Die Entschädigung (Fr. 350.-) orientiert sich an seinem Pendant RT_56_POS_IMMED, ist jedoch Fr. 50.- niedriger.

Die Höhe der Gebühren für EP_59_POS_PERIOD (Art. 67 Bst. c VÜPF) ist die gleiche wie die Gebühren der anderen Überwachungstypen der Notsuche. Analog zur Überwachung ist auch bei der Notsuche die Entschädigung für die periodische Positionsbestimmung höher als für die einmalige Positionsbestimmung. Sie ist jedoch mit Fr. 750.- niedriger als für ihr Pendant der Überwachung RT_57_POS_PERIOD und gleich hoch wie für die übrigen Echtzeitüberwachungen der Notsuche EP_36_RT_CC_IRI (Art. 67 Bst. d VÜPF) und EP_37_RT_IRI (Art. 67 Bst. e).

Für die finanziellen Auswirkungen der neuen Auskunfts- und Überwachungen für Bund, Kantone und MWP siehe oben Ziffer 4.

Weiter wird bei IR_18_ID die Sachüberschrift von «Ausweiskopie» zu «Identitätsnachweis» wie in Artikel 45 VÜPF geändert. Bei IR_21_TECH wird das Wort «Auskunftstyp» in der Spalte «Geschäftsfall» des Anhangs ergänzt, dies analog zu den vier vorherigen Auskunftstypen.

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

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 des Dienstes ÜPF mit den Behörden gemäss Artikel 1 Absatz 2 Buchstaben a-f VÜPF. Als sichere Übertragungsmittel gelten die elektronischen Übertragungsmittel des Verarbeitungssystems 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. 4

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 im neuen Absatz 4 dieselbe Frist auch für Überwachungen des Postverkehrs geregelt. Die Frist für die Übermittlung des Auftrags zur Ausführung einer Echtzeitüberwachung des Postverkehrs an die Anbieterin wird ebenfalls auf eine Stunde festgelegt. Die Überwachungen des Postverkehrs werden lediglich während der Normalarbeitszeiten beauftragt und durchgeführt.

Art. 11 Abs. 2

Der neue *Absatz 2* regelt analog zu den Artikeln 10 Absatz 4, 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. 4).

Art. 12 **Auskunftserteilung**

Die zwei ersten Sätze bleiben unverändert. Der dritte Satz wird in Zusammenhang mit Anpassungen in Artikel 35 Absatz 1 Buchstabe b und c sowie Artikel 40 Absatz 1 Buchstabe b und c VÜPF eingefügt, wonach neu für die Auskunftstypen IR_4_NA und IR_10_Tel der Gültigkeitszeitraum anzugeben ist. Bei den Anbieterinnen werden oft nicht nur die Adresse zum Zeitpunkt der Registrierung, sondern auch Folgeadressen nach einem Umzug und andere Angaben der Kunden, wie z. B. die Adresse oder der Name und Vorname einer anderen Person, die als Zustelladresse gilt, gespeichert. Die Anbieterin hat für den Anfragezeitraum alle ihr bekannten Adressen und Angaben und jeweils den Gültigkeitszeitraum dieser Angaben zu liefern.

Art. 14 Abs 2, 3 und 4

In *Absatz 2* werden die Bearbeitungszeiten für die «grossen» und «mittleren» MWP geregelt. Hierunter fallen die FDA, ausser jene mit reduzierten Überwachungspflichten gemäss Artikel 51 VÜPF(«gross»), die AAKD mit weitergehenden Auskunftspflichten (Art. 22, «mittlere Grösse») und die AAKD mit weitergehenden Überwachungspflichten (Art. 52 VÜPF, «gross»).

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 wenigen Sekunden), da sich die temporären Identifikatoren oft ändern. Diese Auskunft muss daher automatisiert über eine neue Abfrageschnittstelle des Typs LI_HIQR 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 AAKD mit weitergehenden Auskunftspflichten (Art. 22 VÜPF, «mittlere Grösse») von der Auskunftserteilung nach Artikel 48*b* VÜPF befreit sind (s. Art. 18 Abs. 3 VÜPF), das heisst Buchstabe a für sie 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), IR_13_EMAIL (Art. 42), IR_14_EMAIL_FLEX (Art. 27 i. V. mit Art. 42). Die einstündige Frist gilt auch für die folgenden neuen Auskünfte: IR_51_EMAIL_LAST (Auskünfte über E-Mail-Dienste; Art. 42*a* VÜPF), IR_52_COM_LAST (Auskünfte über andere Fernmelde- oder abgeleitete Kommunikationsdienste; Art. 43*a*) und IR_53_ASSOC_PERM: Auskünfte über längerfristig zugeordnete Identifikatoren (Art. 48*a* VÜPF).

Auch 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 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), IR_17_PAY (Art. 44), IR_18_ID (Art. 45), IR_19_BILL (Art. 46), IR_20_CONTRACT (Art. 47), IR_21_TECH

(Art. 48). Neu hinzugekommenist der neu eingeführte Auskunftstyp IR_55_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 Anfrage während einem Wochenende oder einem Feiertag gestellt wurde und daher dringend war. Aus diesem Grund wird *in Ziffer 2* für die «grossen» FDA und AAKD 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. 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 damit die Strafverfolgung nicht behindert werden. Anzumerken ist, dass die AAKD mit weitergehenden Auskunftspflichten (Art. 22 VÜPF, «mittlere Grösse») keinen Pikettdienst zur Verfügung stellen müssen (s. Art. 11 Abs. 1 VÜPF), das heisst Buchstabe c Ziffer 2 für sie nicht anwendbar ist.

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 im IRC einzugeben oder, im Falle einer Störung des IRC, gesichert (s. Art. 3) an den Dienst ÜPF zu senden hat. Anbei einige Beispiele:

Beispiel 1: Ein Auskunftsgesuch wird am Montag um 16.10 Uhr im 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 im 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. 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. Die Behörde hat eine zusätzliche Gebühr (Pikettgebühr) zu entrichten. Der MWP wird eine zusätzliche Entschädigung (Pikettentschädigung) ausgerichtet (s. Art. 6 GebV-ÜPF).

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.

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, welche lediglich die ihnen vorliegenden Angaben zu liefern haben (vgl. Art. 22 Abs. 3 BÜPF), geregelt. 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 Absatz 1 und 68 Absatz 1 VÜPF müssen die Verweise in *Absatz 2* und *Absatz 3* auch angepasst werden.

Anhang 1

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

1) der Auskunftstyp IR_51_EMAIL_LAST, Auskünfte über E-Mail-Dienste (Art. 42*a* VÜPF);
2) der Auskunftstyp IR_52_COM_LAST, Auskünfte über andere Fernmelde- oder abgeleitete Kommunikationsdienste (Art. 43*a* VÜPF)
3) der Auskunftstyp IR_53_ASSOC_PERM, Auskünfte über längerfristig zugeordnete Identifikatoren (Art. 48*a* VÜPF);
4) der Auskunftstyp IR_54_ASSOC_TEMP, sofortige Auskünfte über kurzzeitig zugeordnete Identifikatoren (Art. 48*b* VÜPF);
5) der Auskunftstyp IR_55_TEL_ADJ_NET, Bestimmung der benachbarten Netze bei Telefonie- und Multimediadiensten (Art. 48*c* VÜPF);
6) der Überwachungstyp (Echtzeitüberwachung) RT_56_POS_IMMED, einmalige, sofortige Positionsbestimmung durch das Netzwerk (Art. 56*a* VÜPF);
7) der Überwachungstyp (Echtzeitüberwachung) RT_57_POS_PERIOD, periodisch wiederkehrende Positionsbestimmung durch das Netzwerk (Art. 56*b* VÜPF);
8) der Überwachungstyp (Notsuche) EP_58_POS_IMMED, einmalige, sofortige Positionsbestimmung durch das Netzwerk (Art. 67 Abs. 1 Bst. b VÜPF); sowie
9) der Überwachungstyp (Notsuche) EP_59_POS_PERIOD, periodisch wiederkehrende Positionsbestimmung durch das Netzwerk (Art. 67 Abs. 1 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.

5.4 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 *Buchstabe 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. Bisher konnten sie Zugriffe nur innerhalb ihrer Behörde oder an betroffene Personen und deren Rechtsbeistände vergeben. Neu sollen die Zugriffe auch an die jeweils zuständige genehmigende Behörde, vor allem das Zwangsmassnahmengericht, vergeben werden können. Die im Anhang Ziff. 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.

Neu wird in Absatz 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 festgehaltene 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 beide 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 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[36] die schriftliche Zustimmung der zuständigen Behörde vor. Die Anforderungen an die Schriftlichkeit nach Artikel 14 OR[37] 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, 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,

36 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**)

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

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?), die Dauer und die Faktoren, welche das Fehlerbild kennzeichnen (Welche Überwachungstypen, welche Provider sind betroffen?) untersucht.

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 Daten 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 zu gewährleisten.

Auch in Fällen (*Bst. a Ziff. 2*), wo es unmöglich ist, vorgängig herauszufinden, welche Überwachung ein Problem verursacht oder diese herauszufinden, 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 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 gelieferten Daten guter Qualität kann es dann jedoch zu Qualitätsverlusten kommen oder gar zu Problemen des ganzen V-FMÜ führen. Unter Umständen ist dies nur mit ausführlicheren Analysen der Daten feststellbar und kann somit im Voraus nicht einer konkreten Überwachung zugeordnet werden, so dass keine bestimmte Zustimmung eingeholt werden kann.

Gerade zur Feststellung, welcher Überwachungsauftrag 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. Sollten die Fehlermeldungen eine grosse Anzahl von Überwachungen betreffen, so muss jede Überwachung einzeln auf die Fehlermeldung hin überprüft werden. In einem solchen Fall alle zuständigen Behörden zu eruieren und diese einzeln zu kontaktieren, ist nahezu unmöglich oder mit einem unverhältnismässig hohen Aufwand verbunden. Deshalb ist vorgesehen, dass die Zustimmung auch nicht erforderlich ist, wenn eine grosse Anzahl von Überwachungen betroffen ist (*Bst. b*).

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 Mitarbeiterinnen und Mitarbeiter des Dienstes ÜPF, welche zur Erfüllung ihrer Aufgaben Kenntnis von den Überwachungsdaten nehmen müssen, diese nicht an weitere Personen bekannt geben.

Art. 10 Abs. 4

Die Aufbewahrungsfristen für Daten im V-FMÜ sind in Artikel 11 BÜPF aufgeführt. *Artikel 10 Absatz 4* regelt die Aufbewahrungsdauer der Protokolle, während der diese gespeichert werden. Hier wird das Wort Speicherdauer durch den treffenderen Ausdruck Aufbewahrungsdauer ersetzt.

Allerdings fehlt eine Regelung, wie lange die Protokolle der Löschung der Daten aufbewahrt werden. So soll vor allem nachvollzogen werden können, wann welche Daten gelöscht wurden, die vorher mit verminderten Bearbeitungsfunktionen über einen längeren Zeitraum aufbewahrt wurden. Artikel 10 VDSG[38] kann hier nicht herangezogen werden.

Art. 11 **Massnahmen für die Systemsicherheit**

Der etwas unpräzise und enge Begriff des «ordentlichen Betriebs» wird durch den ebenfalls in Artikel 8 Absatz 4 genannten Begriff «ordnungsgemässen Funktionierens» ersetzt.

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

38 Verordnung vom 14.06.1993 zum Bundesgesetz über den Datenschutz (**VDSG** ; SR **235.11**)

Anhang

Tabelle «Übersicht Bearbeitungszeiten»

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 42 27, 42 42*a* 43*a* 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_13_EMAIL IR_14_EMAIL_FLEX IR_51_EMAIL_LAST IR_52_COM_LAST IR_53_ASSOC_PERM	≤ 1 Stunde	≤ 1 Stunde	≤ 1 Arbeitstag
	48*b*	IR_54_ASSOC_TEMP	sofort	sofort (ausgenommen AAKD mit weitergehenden Auskunftspflichten, Art. 22 VÜPF)	--
	38 39 43 27, 43 44 45 46 47 48 48*c*	IR_8_IP (NAT) IR_9_NAT IR_15_COM IR_16_COM_FLEX IR_17_PAY IR_18_ID IR_19_BILL IR_20_CONTRACT IR_21_TECH IR_55_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

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	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 Stunde	≤ 1 Stunde
Echtzeitüberwachung per Datum während der Bürozeiten	54 55 56 56*a* 56*b* 57 58 59	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 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	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 Stunde	≤ 2 Stunden
Rückwirkende Überwachung während der Bürozeiten	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	≤ 3 Arbeitstage
Rückwirkende Überwachung	60 61	HD_28_NA HD_29_TEL	≤ 1 Stunde	≤ 6 Stunden

in dringenden Fällen (während der Bürozeiten und des Piketts)	62 63 64 65 66	HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV* AS_33_PREP_REF AS_34		
Notsuchen während der Bürozeiten und des Piketts	67 Abs. 1 Bst. a 67 Abs. 1 Bst. b 67 Abs. 1 Bst. c 67 Abs. 1 Bst. d 67 Abs. 1 Bst. e	EP_35_PAGING EP_58_POS_IMMED EP_59_POS_PERIOD EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 Stunde	≤ 1 Stunde
	67 Abs. 1 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. e 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_56_POS_IMMED RT_57_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 58 59 67 Abs. 1 Bst. c	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_57_POS_PERIOD RT_25_TEL_IRI_CC RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI EP_59_POS_PERIOD	≤ 1 Stunde	≤ 1 Arbeitstag

	67 Abs. 1 Bst. d 67 Abs. 1 Bst. e	EP_36_RT_CC_IRI EP_37_RT_IRI		

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

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