Erläuternder Bericht

zur Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11)

A. Ausgangslage

Die Totalrevision des Bundesgesetzes vom 6. Oktober 2000[1] betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) bedingt eine Totalrevision seiner Ausführungsverordnungen, so unter anderem auch der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF).

Der Aufbau der vorliegenden Verordnung folgt der Trennung zwischen allgemeinen Bestimmungen (1. Kapitel), Postverkehr (2. Kapitel), Fernmeldeverkehr (3. Kapitel) und Schlussbestimmungen (4. Kapitel). Der Wunsch nach mehr Rechtssicherheit führte dazu, dass die vorliegende Verordnung die einzelnen Rechte und Pflichten sehr detailliert regelt. So wird in der Verordnung zum Beispiel nicht mehr lediglich zwischen Echtzeit- und rückwirkenden Überwachungstypen unterschieden. Sondern die Verordnung ist so aufgebaut, dass es für jeden angebotenen Dienst eigenständige Bestimmungen gibt, welche jeweils - soweit zutreffend - dessen Überwachung in Echtzeit sowie rückwirkend regeln. Dies führt dazu, dass auch die einzelnen Voraussetzungen eines Auskunfts- beziehungsweise Überwachungstyps sehr detailliert festgelegt sind.

Durch die hohe Regelungsdichte wird nebst der erwünschten Rechtssicherheit das Ziel verfolgt, im Bereich der Fernmeldeüberwachung eine höchstmögliche Standardisierung bei den Auskunfts- und Überwachungstypen zu erreichen und damit die automatischen Abläufe zu begünstigen.

Ein weiterer Unterschied zur VÜPF vom 31. Oktober 2001 bildet des Weiteren der Umstand, dass in der totalrevidierten VÜPF nicht mehr zwischen leitungsvermittelten (CS) und paketvermittelten (PS) Fernmeldediensten differenziert wird. Eine solche Differenzierung ist aufgrund des Technologiewechsels nicht mehr zeitgemäss. So wird zum Beispiel vermehrt über das Internet telefoniert. Neu werden hingegen die einzelnen Überwachungstypen aufgeteilt in Überwachungen von Netzzugangsdiensten (8. Abschnitt und Art. 60) und Überwachungen von Anwendungen (9. Abschnitt und Art. 61-66).

Im Rahmen der Totalrevision des BÜPF wurde zudem der Kreis der Mitwirkungspflichtigen erweitert. So war es beispielsweise nach der bisherigen Gesetzgebung nicht möglich, den nicht meldepflichtigen Fernmeldedienstanbieterinnen und solchen Anbieterinnen, die ihre Kommunikationsdienste über das Internet anbieten, ohne Internetzugangsanbieterin zu sein, die Pflichten im Bereich der Überwachung zu überbinden. Nach der Totalrevision sind im Artikel 2 Buchstabe c BÜPF nun auch Anbieterinnen abgeleiteter Kommunikationsdienste vom persönlichen Geltungsbereich erfasst. Bei den Anbieterinnen abgeleiteter Kommunikationsdienste handelt es sich um solche Anbieterinnen, deren Dienste

[1] SR **780.1**

sich auf Fernmeldedienste stützen und die ihren Benutzerinnen und Benutzern eine Einweg- (z. B. Hochladen eines Dokumentes) oder Mehrwegkommunikation (z. B. Instant Messaging, Chatdienst) ermöglichen. Neu ist zudem, dass der persönliche Geltungsbereich im Bereich der Fernmeldeüberwachung nicht mehr an die vom Fernmeldegesetz[2] in Artikel 4 vorgeschriebene Meldepflicht geknüpft wird. Damit sind auch solche Anbieterinnen vom persönlichen Geltungsbereich erfasst, die nach bisherigem Recht nicht meldepflichtig waren.

Ausgehend von diesen Ausführungen könnte erwartet werden, dass auch die Anzahl der Mitwirkungspflichtigen zunimmt, die Auskunfts- und Überwachungspflichten aktiv auszuführen hätten. Die Zahl solcher Mitwirkungspflichtigen wird jedoch voraussichtlich abnehmen, weil der Bundesrat die im Gesetz vorgesehene Möglichkeit wahrgenommen hat, Anbieterinnen von Fernmeldediensten von gewissen Überwachungspflichten zu befreien, wenn diese Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten. Wir gehen davon aus, dass die Anzahl der gemäss bisherigem Recht aktiv überwachungspflichtigen Fernmeldeanbieterinnen (FDA) von rund 600 auf etwa 20 bis 30 FDA verringern wird. Auch mit der Befreiung von bestimmten Überwachungspflichten soll die Fernmeldeüberwachung weiterhin sichergestellt sein. Die Überwachungen können auch bei FDA mit reduzierten Überwachungspflichten durchgeführt werden, da diese Anbieterinnen immer eine Duldungs- und Zusammenarbeitspflicht haben. Der Dienst ÜPF hat die nötigen Schritte zu unternehmen, damit die Überwachungen weiterhin durchgeführt werden können (Art. 17 Bst. e BÜPF; s. Erläuterungen zu Art. 51.

Den Anbieterinnen abgeleiteter Kommunikationsdienste, die eine Überwachung grundsätzlich zu dulden haben, können hingegen weitergehende Auskunfts- und Überwachungspflichten auferlegt werden, wenn sie Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten (Art. 27 Abs. 3 BÜPF). Hier auch hat der Bundesrat diese Bestimmung präzisiert, und zwar in Artikel 52. Da die Voraussetzungen sehr streng sind, werden zahlenmässig jedoch nicht sehr viele Anbieterinnen abgeleiteter Kommunikationsdienste eine Überwachung aktiv auszuführen haben (s. Ausführungen zu Art. 52) und sehr viele Fernmeldedienstanbieterinnen, die bisher diese Pflicht hatten, werden sie nun nicht mehr haben. Die meisten Anbieterinnen werden lediglich allfällige Überwachungen zu dulden haben, die durch den Dienst ÜPF oder durch von diesem beauftragte Personen durchgeführt werden. Zu diesem Zweck müssen sie unverzüglich Zugang zu ihren Anlagen gewähren. Ausserdem müssen sie die für die Durchführung der Überwachung notwendigen Informationen liefern, die von ihnen angebrachten Verschlüsselungen entfernen und die ihnen zur Verfügung stehenden Randdaten liefern (zum Begriff Randdaten, s. die einleitenden Erläuterungen zum 10. Abschnitt des 3. Kapitels). Trotz Befreiung vieler Anbieterinnen von der aktiven Überwachung, führt dies nicht zu Überwachungslücken, weil der Dienst ÜPF oder durch ihn beauftragte Dritte die angeordneten Überwachungen bei diesen Anbieterinnen ausführen werden. Des Weiteren wird mit der Totalrevision gewissen Bundesstellen ausdrücklich die Möglichkeit eingeräumt, beim Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ein Auskunftsgesuch zu stellen beziehungsweise einen Überwachungsauftrag einzureichen (s. Ausführungen zu Art. 1). So kann neu das

[2] SR **784.10**

Staatssekretariat für Wirtschaft (SECO) ihr Strafantragsrecht einfacher wahrnehmen und unerwünschte Werbeanrufe effektiv bekämpfen, da es aufgrund der neuen Regelung beim Dienst ÜPF Auskünfte über den betreffenden Fernmeldeanschluss verlangen kann. Der Nachrichtendienst des Bundes (NDB) kann nun ebenfalls alle Auskunftstypen beim Dienst ÜPF einholen (s. Art. 15 BÜPF).

Neu soll auch die Qualität der übermittelten Auskunfts- und Überwachungsdaten überprüft werden können, damit der reibungslose Ablauf der Überwachungen nicht beeinträchtigt wird. Die Verordnung legt fest, wann die erforderliche Qualität gewahrt ist und wer die erforderliche Qualität sicherzustellen hat (s. Ausführungen zu Art. 29). Der Dienst ÜPF nimmt dabei die Funktion einer Aufsichtsbehörde wahr und kann bei Nichtbeachtung der gesetzlichen Bestimmungen, beispielsweise der Qualitätsbestimmung, die betreffenden Anbieterinnen gemäss den Vorgaben von Artikel 41 BÜPF oder von Artikel 39 Absatz 1 Buchstabe a BÜPF verwaltungsrechtlich beziehungsweise sogar strafrechtlich sanktionieren.

Um die ordnungsgemässe Ausführung der angeordneten Überwachungen des Fernmeldeverkehrs und der Erteilung von Auskünften sicherzustellen, wird des Weiteren vom Dienst ÜPF das sogenannte Compliance-Verfahren durchgeführt. Es handelt sich hierbei um das Verfahren zur Überprüfung der Auskunfts- und Überwachungsbereitschaft einer Anbieterin (Art. 31-34 BÜPF). Dabei wird überprüft, ob eine auskunfts- beziehungsweise überwachungspflichtige Anbieterin in der Lage ist, nach dem anwendbaren Recht Auskünfte zu erteilen beziehungsweise Überwachungen durchzuführen; siehe Ziffer 2.7 der Botschaft[3] und nachfolgende Ausführungen zu den Artikeln 31-34.

3 BBl **2013** 2747 ff.

B. Erläuterungen zu den einzelnen Artikeln

1. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Einleitung

Art. 1 Gegenstand und Geltungsbereich

Artikel 1 Absatz 1 entspricht dem bisherigen Artikel 1 Absatz 1 VÜPF vom 31. Oktober 2001[4] (Stand 1. Januar 2012).

Absatz 2 präzisiert den persönlichen Geltungsbereich von Artikel 2 BÜPF. Aufgeführt werden wie im bisherigen Artikel 1 VÜPF als Adressaten die anordnenden und die verfahrensleitenden Behörden (in der Regel die Staatsanwaltschaften; *Bst. a*) und die Genehmigungsbehörden (in der Regel die Zwangsmassnahmengerichte; *Bst. b*). Die Polizeibehörden des Bundes, der Kantone und Gemeinden (*Bst. c)* wurden neu eingefügt, um eine abschliessende Liste aller auskunftsberechtigten Stellen aufführen zu können. Die Aufzählung der Adressaten wurde gegenüber der VÜPF vom 31. Oktober 2001[5] aufgrund der Bestimmungen des Artikels 15 Absatz 2 Buchstaben a und b BÜPF um den Nachrichtendienst des Bundes (*Bst. d*) und das Staatssekretariat für Wirtschaft (SECO; *Bst. e*) auf Seiten der auskunftsberechtigten Stellen ergänzt. Hinzu kommen die in Artikel 15 Absatz 1 Buchstabe c BÜPF aufgeführten Behörden des Bundes und der Kantone zwecks Erledigung von Verwaltungsstrafsachen (*Bst. f*). Und schliesslich fällt auch der Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF; *Bst. g*) selbstverständlich in den Geltungsbereich dieser Verordnung.

Eine der wichtigsten Änderungen der Totalrevision des BÜPF besteht in der Erweiterung des Kreises der sogenannten **Mitwirkungspflichtigen**. Damit sind diejenigen Personen gemeint, die dem BÜPF unterstellt sind und denen daraus Pflichten erwachsen, seien es aktive Pflichten, wie die sogenannte Überwachungsbereitschaft (s. Art. 32 BÜPF) oder passive Pflichten, wie die Duldungspflicht (s. Art. 26 Abs. 2 und 6, 27 Abs. 1 und 2, 28 und 29 BÜPF). Die Kategorien von Mitwirkungspflichtigen werden in Absatz 2 Buchstabe h-m wie folgt aufgeführt:

- *Buchstabe h*: Die Anbieterinnen von Postdiensten (PDA) nach dem Postgesetz vom 17. Dezember 2010[6] (PG)[7];

- *Buchstabe i*: Die FDA gemäss Artikel 3 Buchstabe b des Fernmeldegesetzes vom 30. April 1997 (FMG)[8];

- *Buchstabe j*: Die Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen (Anbieterinnen abgeleiteter Kommunikationsdienste)[9];

4 SR **780.11**
5 SR **780.11**
6 SR **783.0**
7 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. a, BBl **2013** 2706 in fine.
8 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. b, BBl **2013** 2707.

- *Buchstabe k*: Die Betreiberinnen von internen Fernmeldenetzen[10];

- *Buchstabe l*: Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen[11];

- *Buchstabe m:* Professionelle Wiederverkäuferinnen von Karten und ähnlichen Mitteln, die den Zugang zu einem öffentlichen Fernmeldenetz ermöglichen[12].

Der Dienst ÜPF wird in der Praxis eine Liste von Diensten erstellen, welche als abgeleitete Kommunikationsdienste wie in Artikel 1 Absatz 2 Buchstabe j aufgeführt gelten, und wird diese Liste regelmässig überprüfen.

Art. 2 Begriffe und Abkürzungen

Artikel 2 orientiert sich an Artikel 2 der VÜPF vom 31. Oktober 2001[13] und führt die Definition der zahlreichen Begriffe und Abkürzungen in einem Anhang auf.

2. Abschnitt: Überwachungsanordnung

Art. 3 Eingaben beim Dienst ÜPF

Absatz 1 befasst sich mit den zugelassenen Übertragungsmitteln für die Einreichung der Überwachungsanordnungen sowie deren Verlängerung und Aufhebung und die Mitteilung der einzurichtenden Zugriffsrechte von den anordnenden Behörden an den Dienst ÜPF.

Die Zugriffsrechte im Verarbeitungssystem des Dienstes ÜPF gelten für die jeweils angeordnete Überwachungsmassnahme und beziehen sich auf die durch die jeweilige anordnende Behörde bezeichneten Mitglieder der Strafverfolgungsbehörden, die mit dem jeweiligen Fall befasst sind und diese Daten im Rahmen der Strafermittlung bearbeiten müssen. Die Zugriffsrechte werden in der Regel zweistufig verwaltet. Jede an Überwachungsmassnahmen beteiligte Strafverfolgungsbehörde bestimmt in der Regel eine für die Verwaltung ihrer Benutzerschaft zuständige Person mit der Funktion Organisationsadministrator (OrgAdmin), welche die Zugriffsrechte innerhalb der Behörde pro Überwachungsmassnahme verwaltet. Der Dienst ÜPF berechtigt die jeweiligen OrgAdmin auf die Überwachungsmassnahme gemäss den Angaben der anordnenden Behörde in der Überwachungsanordnung (s. Art. 49). Der dadurch berechtigte OrgAdmin der Strafverfolgungsbehörde verwaltet dann selbständig die Zugriffsrechte auf die einzelnen Überwachungen für die Mitglieder seiner Behörde im Verarbeitungssystem gemäss den Angaben der anordnenden Behörde (vgl. dazu Art. 8 und 9 der Verordnung vom xx.xx.xxxx[14] über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs [VVS-ÜPF]).

9 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. c, BBl **2013** 2707 in fine.
10 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. d, BBl **2013** 2708 in fine.
11 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. e, BBl **2013** 2709.
12 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. f, BBl **2013** 2709.
13 SR **780.11**
14 SR **XX.XXX**

Alternativ kann eine Strafverfolgungsbehörde die Benutzerverwaltung pro Überwachungsmassnahme auch als Dienstleistung des Dienstes ÜPF beziehen. Der Dienst ÜPF verwaltet in diesem Fall die Zugriffsrechte der einzelnen Benutzenden der jeweiligen Strafverfolgungsbehörde auf die Überwachungsmassnahme gemäss den Angaben der anordnenden Behörde in der Überwachungsanordnung (s. Art. 49).

Falls Änderungen erforderlich sind, welche die Überwachungsmassnahme betreffen (z. B. Änderung oder Hinzufügen eines Überwachungstyps, Änderung des überwachten Adressierungselements aufgrund von Flüchtigkeitsfehlern bei den Strafverfolgungsbehörden), muss die anordnende Behörde eine neue gebührenpflichtige Überwachungsanordnung beim Dienst ÜPF einreichen. Haben der Dienst ÜPF oder die Strafbehörde den Flüchtigkeitsfehler allerdings bemerkt bevor der Auftrag an den Provider übermittelt wurde, dann wird nur für den effektiven Auftrag eine Rechnung gestellt. Änderungen von Zugriffsrechten lösen keine neue Gebühr aus.

Zu den gemäss *Buchstabe a* "durch den Dienst ÜPF zugelassenen sicheren Übertragungsmitteln" zählt zum Beispiel eine elektronische Auftragsschnittstelle gemäss ETSI-Standards wie auch die vom Dienst ÜPF genutzten Verschlüsselungslösungen für E-Mails. Die entsprechenden Vorschriften erlässt das Eidgenössische Justiz- und Polizeidepartement in der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF); siehe auch die Erläuterungen zu Art. 68.

Buchstabe b erlaubt eine alternative Übermittlung der eingangs erläuterten Eingaben der anordnenden Behörden per Post oder Telefax an den Dienst ÜPF. Zu diesem Zweck sind die vom Dienst ÜPF zur Verfügung gestellten Formulare zu verwenden. Diese Übermittlung ist jedoch nur erlaubt, falls technische Gründe eine Übermittlung gemäss Buchstabe a verhindern. Die Strafverfolgungsbehörden haben alles daran zu setzen, dass sie zur Übermittlung gemäss Buchstabe a in der Lage sind.

Buchstabe c hält fest, dass nach einer telefonischen Anordnung, welche nur in dringlichen Fällen (z. B. Notsuchen, Fahndungen, Anordnungen ausserhalb der Normalarbeitszeiten) zulässig ist, die Anordnung mit einem Übertragungsmittel gemäss Buchstabe a oder b nachgereicht werden muss.

Gemäss *Absatz 2* sollen die Übertragungsmittel gemäss Absatz 1 Buchstabe a durch einen Online-Zugriff auf das Verarbeitungssystem des Dienstes ersetzt werden. Dies vereinfacht den anordnenden Behörden die Eingaben beim Dienst ÜPF erheblich, weshalb der Zeitpunkt durch diesen bestimmt werden soll, ab welchem die Eingaben nur noch über den Online-Zugriff eingereicht werden.

Art. 4 Durchführung der Überwachung

Artikel 4 entspricht im Wesentlichen dem Artikel 17 Absatz 1 und 6 der VÜPF vom 31. Oktober 2001[15] und regelt die Durchführung der Überwachung.

Absatz 1 entspricht der bisherigen Regelung.

Sollte die Mitwirkungspflichtige auf Grund betrieblicher Probleme nicht in der Lage sein, ihre Pflichten zur Überwachung des Post- und Fernmeldeverkehrs

15 SR **780.11**

wahrzunehmen, muss sie dies gemäss *Absatz 2* neu dem Dienst ÜPF nicht nur unverzüglich melden, sondern hat zusätzlich eine schriftliche Begründung nachzuliefern. Betriebliche Probleme schliessen sowohl technische, als auch organisatorische Gründe ein. Diese Probleme können Konsequenzen haben (z. B. Art. 33 Abs. 5 und Art. 34 Abs. 1 BÜPF).

Es ist wichtig, dass die Mitwirkungspflichtige unverzüglich den Dienst ÜPF über alle Probleme informiert, welche die zeitkritischen Überwachungen beziehungsweise Überwachungsaufträge betreffen. Daher hat diese Meldung sofort telefonisch an die entsprechenden Kontaktstellen des Dienstes ÜPF zu erfolgen. Falls die Mitwirkungspflichtige nicht in der Lage sein sollte, einen Überwachungsauftrag auszuführen oder ihre Pflichten bei der Durchführung von Echtzeitüberwachungen zu erfüllen, hat sie den zuständigen Bereich des Dienstes ÜPF innerhalb der Bürozeiten über dessen zentrale Telefonnummer beziehungsweise ausserhalb der Bürozeiten über dessen Pikettnummer zu kontaktieren. Die Mitwirkungspflichtige hat dem Dienst ÜPF die Störungsmeldung in schriftlicher Form unter Angabe des genauen Ausfallzeitraums, der Problembeschreibung, einer chronologischen Übersicht der eingeleiteten Massnahmen und des Problemstatus am nächsten Arbeitstag zukommen zu lassen. Falls die Störung zu diesem Zeitpunkt noch nicht behoben ist, hat sie ausserdem dem Dienst ÜPF nach der Störungsbehebung eine gleichartige schriftliche Abschlussmeldung zu senden. Im Gegenzug hat auch der Dienst ÜPF die Mitwirkungspflichten unverzüglich zu informieren, sollte er infolge betrieblicher Probleme auf seiner Seite nicht in der Lage sein Überwachungen auszuführen.

Im Falle solcher Störungen und unabhängig davon, auf welcher Seite die Probleme aufgetreten sind, hat die Mitwirkungspflichtige gemäss *Absatz 3* mindestens die Randdaten der Echtzeitüberwachung während der in den technischen Vorschriften des EJPD angegebenen Zeitspanne zwischenzuspeichern und unverzüglich nachzuliefern (zum Begriff *Randdaten der Echtzeitüberwachung* s. die einleitenden Erläuterungen des 3. Kapitels 10. Abschnitt). Falls die Randdaten der Echtzeitüberwachung nicht mehr verfügbar oder unvollständig sein sollten, hat die Mitwirkungspflichtige gemäss den Anweisungen des Dienstes ÜPF unverzüglich die entsprechenden Randdaten der rückwirkenden Überwachung zu liefern (zum Begriff *Randdaten der rückwirkenden Überwachung* s.die einleitenden Erläuterungen des 3. Kapitels 10. Abschnitt).

Art. 5 Schutz von Amts- und Berufsgeheimnissen

Artikel 5 entspricht den Artikeln 17 Absatz 2 (Überwachung der Telefondienste) und 25 Absatz 2 (Überwachung des Internets) VÜPF vom 31. Oktober 2001[16] und hat den Schutz des Amts- und Berufsgeheimnisses zum Ziel. Diese Bestimmung regelt nur die Situation, wenn der Dienst ÜPF feststellt, dass die Überwachung einen Amts- oder Berufsgeheimnisträger betrifft, ohne dass Vorkehren gemäss Artikel 271 StPO[17] beziehungsweise Artikel 70*b* MStP[18] getroffen worden sind (*Buchstaben a und b*).

Gemäss Artikel 16 Buchstabe e BÜPF setzt der Dienst ÜPF die von der Genehmigungsbehörde angeordneten Vorkehren zum Schutz von Amts- und

16 SR **780.11**
17 SR **312.0**
18 SR **322.1**

Berufsgeheimnissen um. Diese Aufgabe wird auf die Überwachung des Postverkehrs ausgeweitet, da sie auch in diesem Bereich durchaus sinnvoll ist. Diese Bestimmung muss zu den Artikeln 271 und 274 Absatz 4 Buchstabe a StPO sowie zu den Artikeln 70*b* und 70*e* Absatz 4 Buchstabe a MStP in Beziehung gesetzt werden. In diesen Artikeln wird die auf die Überwachung anwendbare Regelung erwähnt, falls ein Amts- oder Berufsgeheimnis geschützt werden muss, von dem die Strafverfolgungsbehörde keine Kenntnis erhalten darf. Der Dienst trifft die notwendigen Vorkehren für die Umsetzung der Massnahmen, die im Rahmen der oben aufgeführten Artikel beschlossen wurden; er nimmt aber zum Beispiel nicht selbst die Aussonderung vor, die in diesen Artikeln erwähnt ist (Art. 271 StPO und Art. 70*b* MStP)"[19].

Gemäss Artikel 15 Buchstabe j und k (Postverkehr) beziehungsweise gemäss Artikel 49 Absatz 1 Buchstaben k und l (Fernmeldeverkehr) muss die beim Dienst ÜPF eingereichte Überwachungsanordnung den Vermerk betreffend die Personen, die einem Amts- oder Berufsgeheimnis gemäss Artikel 271 StPO oder gemäss Artikel 70b MStP unterstehen, sowie die Vorkehrungen zu deren Schutz, enthalten; siehe auch Artikel 9 Absatz 2 Buchstabe i, wonach die Unterlagen zu den besonderen angeordneten Schutzmassnahmen Teil der Überwachungsakte sind.

Gemäss BÜPF kann der Dienst ÜPF die ihm übermittelten Überwachungsanordnungen nicht nur einer formellen Prüfung, sondern auch einer materiellen Prüfung unter dem Gesichtspunkt des Verwaltungsrechts unterziehen[20]. Im Rahmen dieser Prüfung könnte der Dienst ÜPF eine entsprechende Feststellung machen, so z. B. wenn die Berufsbezeichnung einen Hinweis auf einen entsprechenden Beruf gibt und keine Schutzmassnahmen angeordnet wurden.

Soll beispielsweise ein Arzt überwacht werden, welcher dem Arztgeheimnis untersteht, ohne dass Vorkehrungen gemäss Artikel 271 StPO oder gemäss Artikel 70b MStP angeordnet worden sind, so wird die Überwachung zwar durch den Dienst ÜPF ausgeführt, die anordnende Behörde erhält jedoch vorerst keinen Zugriff auf die aufgezeichneten Daten. Die anordnende Behörde sowie die Genehmigungsbehörde werden entsprechend darüber orientiert. Die Genehmigungsbehörde hat die Möglichkeit, die Überwachung unter Auflage einer Aussonderung von Informationen (Triage) gemäss Artikel 271 Absatz 1 und 274 Absatz 4 Buchstabe a StPO oder gemäss Artikel 70b und 70e Absatz 4 Buchstabe a MStP zu genehmigen. Sie kann einen Verantwortlichen ernennen, welcher die Daten vorgängig sichtet und eine entsprechende Triage vornimmt. Wird ein Verantwortlicher ernannt, wird diesem durch den Dienst ÜPF die Berechtigung und/oder der Zugriff auf die entsprechenden Daten im Verarbeitungssystem erteilt. Dem Dienst ÜPF wird dann durch die Genehmigungsbehörde mitgeteilt, auf welche Daten die anordnende Behörde Zugriff erhalten soll. Wurde eine Triage angeordnet, so erhält der Dienst ÜPF von der Genehmigungsbehörde regelmässig eine entsprechende Liste und nimmt die Triage im Verarbeitungssystem vor. Das heisst, die anordnende Behörde erhält auf die von der Genehmigungsbehörde ausgewählten Daten Zugriff und die restlichen Daten werden durch den Dienst ÜPF vernichtet[21]. Dieser Vorgang gilt für die gesamte Überwachungsdauer.

19 BBl **2013** 2725 in fine und 2726 in initio; siehe auch die Erläuterungen in der Botschaft zum BÜPF zu Art. 271 StPO und 70*b* MStP.
20 BBl **2013** 2696; Ziff. 1.4.5.
21 BBl **2006** 1249

Buchstabe c hält fest, dass das Vorerwähnte für den Nachrichtendienst des Bundes als anordnende Behörde sinngemäss gilt. In diesem Fall ist die Genehmigungsbehörde das Bundesverwaltungsgericht.

Art. 6 Geheimhaltungspflicht

Artikel 6 entspricht dem Artikel 17 Absatz 7 und Artikel 25 Absatz 7 VÜPF vom 31. Oktober 2001[22] und regelt die Geheimhaltungspflicht.

Die Geheimhaltungspflicht ist insbesondere für den Erfolg der Überwachungsmassnahmen und Auskünfte sowie für den Schutz der Persönlichkeitsrechte der betroffenen Personen von besonderer Wichtigkeit und darf keinesfalls in irgendeiner Weise verletzt werden. Weder die betroffene Person noch unbefugte Dritte dürfen direkt oder indirekt Hinweise über Überwachungen oder Auskunftserteilungen erhalten (s. a. Art. 320 StGB und Art. 39 Abs. 1 Bst. d BÜPF).

Art. 7 Technische Datensortierung (Filterung)

Artikel 7 führt die Bestimmung von Artikel 17 Buchstabe g BÜPF weiter aus.

Die vorgesehene Sortierung unterscheidet sich von der Aussonderung (Triage) gemäss Artikel 271 StPO und 70*b* MStP in Zusammenhang mit dem Schutz des Amts- und Berufsgeheimnisses (s. o. ad Art. 5).

Unter technischer Datensortierung (Filterung) ist zu verstehen, dass die auszuwertende Datenmenge entsprechend den dokumentierten Anweisungen der anordnenden Behörde mittels automatischer Verfahren reduziert wird. Die anordnende Behörde kann die automatisierte Filterung der Überwachungsdaten verfügen, um beispielsweise die Auswertung grosser Datenmengen zu erleichtern. Dabei werden für die Ermittlungen irrelevante Daten, wie etwa Internet-TV, die keinen Erkenntnisgewinn für die Strafbehörden darstellen, bereits vor der Speicherung im Verarbeitungssystem aus dem Datenstrom herausgefiltert, so dass sie gar nie im Verarbeitungssystem gespeichert werden.

Hiermit sind nicht die Fälle gemeint, wenn viele unbeteiligte Dritte von einer Überwachungsmassnahme betroffen sind (z. B. zentrale Telefonnummer einer Firma soll überwacht werden). Auch in solchen Fällen nimmt der Dienst ÜPF mit der anordnenden Behörde Rücksprache (sinngemäss wie in Art. 5).

Die Filterung wird durch den Dienst ÜPF kostenlos unter der Voraussetzung durchgeführt, dass sie automatisiert und mit verhältnismässigem Aufwand erfolgen kann. Unter verhältnismässigem Aufwand ist zu verstehen, dass der Dienst ÜPF im Rahmen der ihm zur Verfügung stehenden finanziellen, personellen und technischen Ressourcen die entsprechenden Vorkehrungen treffen kann. Falls der Dienst ÜPF feststellt, dass die gewünschte Filterung technisch unmöglich ist oder sie sich nicht mit verhältnismässigem Aufwand realisieren lässt, teilt er dies der anordnenden Behörde unverzüglich und begründet mit.

Die Strafverfolgungsbehörden haben die Verantwortung für die Konfiguration der vom Dienst ÜPF vorgegebenen Filtermöglichkeiten. Der Dienst ÜPF berät sie dabei. Aufgrund der hohen Anforderungen an die Durchführung dieser Filterung

22 SR **780.11**

kommen nur automatisierte Verfahren zur Anwendung. Jede andere Art der Filterung wäre sehr kompliziert oder gar nicht realisierbar[23]. Die anordnende Behörde nimmt vor der Anordnung einer technischen Datensortierung Rücksprache mit dem Dienst ÜPF bezüglich deren Machbarkeit.

Art. 8 Aufzeichnung der Telefonate zu Beweiszwecken

Artikel 8 Absatz 1 ermöglicht es dem Dienst ÜPF, zu Beweiszwecken die im Zusammenhang mit der Erfüllung seiner Aufgaben getätigten Telefonate aufzuzeichnen. Dies geschieht aufgrund der Tatsache, dass die anordnenden Behörden Überwachungsaufträge (z. B. in dringlichen Fällen; s. Art. 3 Abs. 1 Bst. c) beziehungsweise Erläuterungen zu Überwachungsaufträgen oft telefonisch erteilen. Vereinzelt kam es in der Vergangenheit bei nachträglichen Abklärungen zu unterschiedlichen Aussagen der Mitarbeitenden des Dienstes ÜPF und der anordnenden Behörden betreffend telefonisch in Auftrag gegebener Überwachungsmassnahmen. Im Rahmen von Untersuchungen ist es notwendig, die Fakten einwandfrei feststellen zu können. Deshalb ist es wichtig, dieses Beweisführungsmittel an der Hand zu haben. Zudem werden bereits alle *schriftlichen* Kommunikationen zwischen Dienst ÜPF, Behörden und Mitwirkungspflichtigen aufbewahrt, zum Beispiel Anordnungen, Verfügungen, Überwachungsaufträge, Korrespondenzen (s. Art. 9 Überwachungsakte). Die gleiche Regelung soll nun auch für telefonische Kommunikationen gelten. Die Aufzeichnung der Telefonate betrifft die Büronummer und die Pikettnummer des Überwachungsmanagements des Dienstes ÜPF.

Eine allfällige Auswertung der Aufzeichnungen ist nur durch den Datenschutzbeauftragten des Dienstes ÜPF möglich (*Abs. 2*).

Der Dienst ÜPF darf die Aufzeichnungen nur während zwei Jahren aufbewahren (*Abs. 3*). Sie sind nach Ablauf der Aufbewahrungsfrist zu vernichten.

Art. 9 Überwachungsakte

Artikel 9 regelt die Aktenführung des Dienstes ÜPF und führt abschliessend den Inhalt der Überwachungsakte auf.

Absatz 1 verpflichtet den Dienst ÜPF zur Anlegung einer Akte für jede Überwachungsanordnung im Verarbeitungssystem gemäss VVS-ÜPF. Diese Anordnung kann mehrere Überwachungsmassnahmen umfassen.

Absatz 2 hält fest, welche Unterlagen die Überwachungsakte umfasst. Dies sind die Überwachungsanordnung sowie allfällige Beilagen, der Überwachungsauftrag beziehungsweise die Überwachungsaufträge an die entsprechenden Mitwirkungspflichtigen, die Bestätigung beziehungsweise Bestätigungen, wann der Auftrag durch den Dienst ÜPF an die Mitwirkungspflichtigen erteilt wurde, die Quittierung (Datum und Uhrzeit) der Mitwirkungspflichtigen über die Ausführung des Überwachungsauftrags beziehungsweise der Überwachungsaufträge, die Verfügung beziehungsweise Verfügungen der Genehmigungsbehörde sowie allfällige Beschwerdeentscheide, allfällige Verlängerungsanordnungen und Verfügungen der Genehmigungsbehörde, die Aufhebungsanordnung beziehungsweise Aufhebungsanordnungen, allfällige zu der Massnahme ergangene

23 BBl **2013** 2728

Korrespondenz (E-Mails etc.), allfällige besondere angeordnete Schutzmassnahmen (beispielsweise Triage) sowie die Rechnungsunterlagen.

Diese Akte bildet auch die Grundlage für die Gebührenerhebung gegenüber der anordnenden Behörde und die an die beauftragten Mitwirkungspflichtigen zu leistenden Entschädigungszahlungen.
Es besteht das Ziel, die Überwachungsakten elektronisch und nach Möglichkeit im Verarbeitungssystem aufzubewahren.

Absatz 3 regelt die Aufbewahrung der Überwachungsdaten gemäss Artikel 11 BÜPF und die Vernichtung der Überwachungsdaten gemäss Artikel 14 VVS-ÜPF.

3. Abschnitt: Arbeitszeiten und Pikett-Regelung

Art. 10 Normalarbeitszeiten und Feiertage

Artikel 10 ist neu und definiert in *Absatz 1* die Normalarbeitszeiten. Diese entsprechen der aktuellen Praxis. Die Uhrzeiten beziehen sich auf Schweizer Zeit.

Absatz 2 definiert die Feiertage. Diese entsprechen denjenigen von Artikel 66 Absatz 2 der Bundespersonalverordnung vom 3. Juli 2001[24].

Art. 11 Leistungen ausserhalb der Normalarbeitszeiten

Artikel 11 ist neu, entspricht aber der aktuellen Praxis des Dienstes ÜPF. Er regelt die Leistungen des Dienstes ÜPF sowie der Mitwirkungspflichtigen im Pikettdienst. Dringende Aufträge werden im Pikettdienst nur nach telefonischer Avisierung über die Pikettnummer des Dienstes ÜPF erledigt.

In *Absatz 1* werden die Leistungen des Dienstes ÜPF im Pikettdienst abschliessend aufgeführt.

Es folgt, dass insbesondere keine besonderen Auskünfte und Überwachungen (sog. Spezialfälle) im Pikettdienst erbracht werden. Dies sind Auskünfte beziehungsweise Überwachungen, die keinem Auskunfts- beziehungsweise Überwachungstyp der Verordnung entsprechen (sog. nicht-standardisierte Auskünfte bzw. Überwachungen); vergleiche dazu auch die Ausführungen zu den Artikeln 23 und 26. Im Pikettdienst kann der Dienst ÜPF insbesondere keine Schulungen erbringen und nur eine eingeschränkte Beratung leisten.

Absatz 2 legt die Anbieterinnen fest, die den Dienst ÜPF ausserhalb der Normalarbeitszeiten unterstützen müssen. Zum Pikettdienst verpflichtet sind die FDA sowie die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten gemäss Artikel 51. Auf Grund der Verhältnismässigkeit sind die FDA mit reduzierten Überwachungspflichten (Art. 50) sowie die Anbieterinnen abgeleiteter Kommunikationsdienste ohne weitergehende Überwachungspflichten (d. h. diejenigen, die die Voraussetzungen von Art. 51 nicht erfüllen) von diesen Pflichten befreit. Somit können Massnahmen, die solche Anbieterinnen betreffen, nicht im Pikett ausgeführt werden. Von den Pikettpflichten befreit sind auch die PDA.

24 SR **172.220.111.3**

Besondere Auskünfte und Überwachungen gemäss Artikel 25 stellen sogenannte Spezialmassnahmen dar, welche vom Dienst ÜPF oder durch von diesem beauftragte Personen durchgeführt werden. Da für deren Durchführung mehr Zeit benötigt wird und da diese erheblich komplexer sind sowie meist mehrere Personen zusammen arbeiten müssen, sieht *Absatz 3* vor, dass im Pikett weder die Anordnung besonderer Überwachungen noch die Gesuche um besondere Auskünfte entgegengenommen und erbracht werden.

4. Abschnitt: Statistiken

Art. 12 Statistik über Überwachungsmassnahmen und Auskünfte

Gemäss BÜPF vom 6. Oktober 2000 führte der Dienst ÜPF bereits eine Statistik über die Überwachungsmassnahmen. Da die Übergangsbestimmungen (Art. 74 Abs. 6 Bst. a VÜPF) vorsehen, dass der Dienst ÜPF die Statistiken (Art. 12) während der Übergangszeit noch nach bisherigem Recht erstellen kann, wird hier noch auf diese Bestimmungen eingegangen: Artikel 11 Absatz 1 Buchstabe f BÜPF vom 6. Oktober 2000 ist dabei die Rechtsgrundlage für die Statistik über die Überwachung des Postverkehrs und Artikel 13 Absatz 1 Buchstabe j BÜPF vom 6. Oktober 2000 diejenige für die Statistik über die Überwachung des Fernmeldeverkehrs.

Artikel 16 Buchstabe k BÜPF vom 18. März 2016 wurde am 10. März 2014 durch den Ständerat eingeführt und sieht vor, dass der Dienst ÜPF weiterhin eine Statistik über die Überwachungen führt.

Weitere Bestimmungen zur Statistik befinden sich in den Artikeln 35 Absatz 3 BÜPF vom 18. März 2016 (Notsuche) und 36 Absatz 2 BÜPF vom 18. März 2016 (Fahndung nach verurteilten Personen). Die VÜPF vom 31. Oktober 2001 enthält keine Bestimmungen zur Statistik. Auf der Website des Dienstes ÜPF (www.li.admin.ch > Statistik) sind die Statistiken seit 2010 abrufbar. Dabei wird zwischen den Überwachungsmassnahmen, welche im Rahmen eines Strafverfahrens angeordnet werden, und den Notsuchen nach vermissten Personen unterschieden.

Während der Revisionsarbeiten an der VÜPF zeigte sich, dass die heutige Praxis in dieser Verordnung zu verankern ist; dies unter Berücksichtigung von Neuerungen. Grundsätzlich ist es von öffentlichem Interesse zu wissen, welche Art von Überwachungen und wie viele pro Jahr durchgeführt werden sowie was sie kosten.

Gemäss *Absatz 1* sind die vom Dienst ÜPF erstellten Statistiken einmal jährlich, in der Regel zu Beginn des Jahres, zu veröffentlichen. Die Veröffentlichung erfolgt im Internet auf der Webseite des Dienstes ÜPF (www.li.admin.ch). Eine Veröffentlichung in anderen Medien (TV, Radio, Zeitungen etc.) ist ebenfalls möglich.

Absatz 2 hält fest, was die Statistiken enthalten müssen. *Buchstaben a-c* entsprechen der bisherigen Praxis. Einzig die Fahndung in *Buchstabe c* wird neu aufgeführt. *Buchstaben d-f* enthalten Neuerungen. In *Buchstabe b* wird das Fürstentum Lichtenstein auch erwähnt, da es als zuständige Behörde im Sinne von Artikel 35 BÜPF betrachtet werden kann, um Notsuchen anzuordnen (s. Ziff. 3 des

Notenaustauschs vom 27. Oktober 2003[25]). In *Absatz 2* wurde auf eine Bestimmung zur Anzahl der nicht genehmigten Überwachungen verzichtet (wie ANITA FETZ und STEFAN ENGLER am 10.03.2014 verlangten; BO 2014 S 112). Zurzeit wären nur die Zwangsmassnahmengerichte in der Lage, solche Statistiken zu liefern, nicht jedoch der Dienst ÜPF, da dieser nur von solchen nicht genehmigten Überwachungsmassnahmen erfährt, die ihm seitens der Staatsanwaltschaft vor dem Entscheid des Zwangsmassnahmengerichts überhaupt zugestellt wurden. Vermutlich gibt es aber eine nicht unwesentliche Anzahl von Überwachungsmassnahmen, die vom Zwangsmassnahmengericht abgelehnt werden, bevor sie beim Dienst ÜPF eintreffen, wovon er naturgemäss keine Kenntnis erhält.

Der Dienst ÜPF ist auch nicht in der Lage, Hinweise auf den Erfolg der Überwachungsmassnahmen zu geben (s. Anfrage ALINE TREDE 15.5191 "Überwachung des Post und Fernmeldeverkehrs. Wirksamkeit der Vorratsdatenspeicherung" und der Antwort des Bundesrates vom 16.03.2015).

Bei der Redaktion dieses Artikels stellte sich die Frage, ob diejenigen Überwachungen zu zählen sind, welche im vergangenen Jahr angeordnet oder diejenigen, die abgeschlossen wurden. Die bisherige Praxis soll nun weitergeführt und alle im vergangenen Jahr angeordneten Überwachungen gezählt werden. Allerdings besteht ein Problem für die Fristberechnung (*Abs. 2 Bst. d*) bei Überwachungen, die in zwei aufeinanderfolgenden Kalenderjahren laufen. Dort ist es nicht möglich, zu Beginn des Jahres bei der Erstellung der Statistiken die Gesamtdauer der im Vorjahr angeordneten Überwachungen zu kennen, wenn diese noch nicht beendet sind. Dieses Problem wird in der Praxis noch zu lösen sein.

Art. 13 Statistik über Überwachungsmassnahmen mit besonderen technischen Geräten und besonderen Informatikprogrammen

In Bezug auf den Einsatz von besonderen technischen Geräten (bspw. IMSI-Catcher) und besonderen Informatikprogrammen (sogenannte "GovWare") stellt Artikel 13 die Ausführungsbestimmung der neuen Artikel 269*bis* Absatz 2 und 269*ter* Absatz 4 StPO für die Staatsanwaltschaften beziehungsweise der neuen Artikel 70*bis* Absatz 2 und 70*ter* Absatz 4 MStP für die militärischen Untersuchungsrichter dar. Diese neuen Bestimmungen sehen vor, dass der Bundesrat die Einzelheiten regelt. Grundsätzlich sollten sie in den Ausführungsbestimmungen der StPO beziehungsweise in denjenigen der MStP (z. B. in der MStV[26]) zu finden sein. Allerdings kennt das heutige Strafverfahrensrecht keine allgemeine Verordnung im Bereich des Strafverfahrens. Eine neue Verordnung nur zu diesem Zweck zu erstellen, wäre weder angemessen noch verhältnismässig. In Anbetracht, dass die besonderen technischen Geräten und die besonderen Informatikprogramme im weiteren Sinne in Zusammenhang mit der Materie der Überwachung stehen, die im BÜPF und der VÜPF geregelt ist und dass es effizienter ist, die Veröffentlichung dieser Statistiken zu zentralisieren, erscheint es sinnvoll, die Kompetenz, diese Statistiken zu publizieren, dem Dienst ÜPF zu überlassen und die Bestimmungen in der VÜPF aufzunehmen; dies erfolgt mit der Schaffung von Artikel 13.

25 SR **0.780.151.41**
26 SR **322.2**

Die Statistiken werden durch die verschiedenen kantonalen Strafverfolgungsbehörden, die Staatsanwälte des Bundes und die verschiedenen militärischen Untersuchungsrichter geführt. Letztere melden diese dem zuständigen Oberauditorat. Deshalb sieht *Absatz 2* vor, dass die von den verschiedenen öffentlichen Behörden erstellten Statistiken dem Dienst ÜPF zu übermitteln sind. Das heisst, die kantonalen Staatsanwaltschaften, die Bundesanwaltschaft und das Oberauditorat haben ihre Statistiken dem Dienst ÜPF zuzustellen. Die Übermittlung muss im ersten Quartal des Folgejahres stattfinden, so dass der Dienst ÜPF alle Statistiken zusammen innert nützlicher Frist publizieren kann.

Im Vorfeld wurden einige Vorbehalte über die Notwendigkeit der Veröffentlichung zum Ausdruck gebracht. Es wurde befürchtet, dass die Veröffentlichung den reibungslosen Ablauf der Ermittlungen gefährden könnte, da die Verwendung von besonderen technischen Einrichtungen zur Überwachung, vor allem aber von GovWare, viel seltener ist als die normalen Überwachungsmassnahmen. Veröffentlichte Statistiken der Kantone, auch wenn diese anonymisiert werden, könnten Rückschlüsse ermöglichen, um welches Strafverfahren es sich handelt, dies vor allem in den kleinen Kantonen. Diese Bedenken sind nachvollziehbar. *Absatz 2 Satz 2* sieht deshalb vor, dass die Statistiken den Einsatz von besonderen technischen Geräten oder besonderen Informatikprogrammen nicht enthalten, wenn deren Einsatz noch nicht abgeschlossen ist. Die kantonalen Strafverfolgungsbehörden oder die Bundesanwaltschaft haben den Dienst ÜPF über das Ende der Überwachungsmassnahme zu orientieren. Damit kann diese vom Dienst ÜPF in der nächsten Statistik berücksichtigt werden.

Absatz 3 hält fest, dass der Dienst ÜPF jährlich eine konsolidierte Statistik publiziert. Die Angaben zum Kanton der anordnenden Behörde und die Angaben zur anordnenden Behörde des Bundes werden in der Statistik nicht aufgeführt, um eben die Befürchtungen zu beseitigen, dass mit diesen Informationen Ermittlungen beziehungsweise zukünftige Ermittlungen gefährdet werden könnten.

Bei Überwachungsmassnahmen mit besonderen technischen Geräten und besonderen Informatikprogrammen gibt es keine Gebühren und Entschädigungen. Die Möglichkeiten der Ausweisung der Kosten solcher Überwachungsmassnahmen wurden untersucht. Besondere Informatikprogramme müssen in der Regel nach der Beschaffung immer wieder an den speziellen Einsatzfall angepasst werden oder es kommen Einzelentwicklungen zum Einsatz. Je nach Kostenmodell können zu den einmaligen Beschaffungskosten und den wiederkehrenden Betriebskosten auch noch Lizenzgebühren für jeden Einsatzfall hinzukommen. Des Weiteren entstehen Kosten für den Personaleinsatz zur Vorbereitung des Aufbringens der GovWare (z. B. Polizeikräfte, Informatiker, Übersetzer). Da die korrekte Ausweisung der Kosten pro Einsatzfall einen sehr hohen Aufwand verursachen würde, wird auf die Angabe der Kosten in dieser Statistik verzichtet.

2. Kapitel: Postverkehr

Art. 14 Pflichten der PDA

Artikel 14 entspricht im Wesentlichen dem Artikel 14 der VÜPF vom 31. Oktober 2001[27] und regelt die Pflichten der Anbieterinnen von Postdiensten (PDA); siehe auch Artikel 19 BÜPF (Pflichten der Anbieterinnen von Postdiensten), Artikel 20 BÜPF (Informationen vor Anordnung einer Überwachung), die Botschaft zum BÜPF zu dieser Bestimmung[28] und die Erläuterungen hier unten ad Artikel 16.

Absatz 1 regelt welche Überwachungen die PDA auszuführen haben; *Absatz 2* vor allem die Zeiten der Erreichbarkeit.

Art. 15 Anordnung zur Überwachung des Postverkehrs

Artikel 15 entspricht im Wesentlichen dem Artikel 11 der VÜPF vom 31. Oktober 2001[29] und regelt den Inhalt der Überwachungsanordnung im Falle einer Überwachung des Postverkehrs (für den Fernmeldeverkehr, s. u. Erläuterungen zu Art. 48).

Für die *Buchstaben j* und *k*, siehe die Erläuterungen zu Artikel 5 (Schutz von Amts- und Berufsgeheimnissen).

Art. 16 Überwachungstypen

Artikel 16 entspricht im Wesentlichen dem Artikel 12 VÜPF vom 31. Oktober 2001[30] und regelt die verschieden Überwachungstypen im Postverkehr.

Die Lieferumfänge der einzelnen Überwachungstypen sind im Wesentlichen gleich geblieben. Neu ist lediglich, dass im Rahmen der Echtzeitüberwachung auch der Aufgabeort der Postsendung (vgl. Bst. b Ziff. 4) und die Unterschrift des Empfängers (vgl. Bst. b Ziff. 6), soweit verfügbar, anzugeben sind. Beim Empfänger kann es sich um die Adressatin beziehungsweise den Adressaten der Postsendung handeln, wie jedoch auch eine Dritte zur Entgegennahme der Sendung berechtigte Person. Zu erwähnen ist, dass die Pflicht zur Speicherung und Lieferung von Randdaten - wie nach der bisherigen Regelung - nur im Falle von Postsendungen mit Zustellnachweis besteht. Ein Zustellnachweis im Sinne der Verordnung ist sicherlich gegeben bei Produkten wie eingeschriebenen Postsendungen sowie bei Paketen mit "Track and Trace". Haben die PDA weitere Daten hinterlegt, haben sie auch diese auf Anfrage zu liefern (vgl. Bst. c Ziff. 2).

Angemerkt sei noch, dass die elektronischen Kommunikationsdienste der PDA unter die Fernmeldeüberwachung fallen, beispielsweise E-Mail-Dienste der Post wie PostMail.

27 SR **780.11**
28 BBl **2013** 2729-2731
29 SR **780.11**
30 SR **780.11**

3. Kapitel: Fernmeldeverkehr

Aufgrund des raschen technischen Fortschritts und der vielfältigen Implementierungsmöglichkeiten bei den Mitwirkungspflichtigen sind für die zahlreichen Dienste, Optionen und Parameter der Auskunfts- und Überwachungstypen abschliessende Aufzählungen nicht geeignet und es werden stattdessen typische Beispiele aufgeführt.

Der Detaillierungsgrad der Verordnung hat sich im Vergleich zur bisherigen Verordnung stark erhöht und kommt damit dem Wunsch nach mehr Rechtssicherheit entgegen.

1. Abschnitt: Allgemeine Bestimmungen für Auskünfte und Überwachungen

Art. 17 Auskunftsgesuche

In diesem Artikel wird geregelt, wie die Einreichung der Auskunftsgesuche durch die gemäss Artikel 15 BÜPF berechtigten Behörden an die 3 Kategorien von Mitwirkungspflichtigen (FDA, Anbieterinnen abgeleiteter Kommunikationsdienste und Betreiberinnen interner Fernmeldenetze) sowie die Übermittlung der erteilten Auskünfte zurück an die Behörden zu erfolgen haben. Der Dienst ÜPF betreibt ein Verarbeitungssystem, das unter anderem auch die Übermittlung der Auskunftsgesuche und der erteilten Auskünfte übernimmt (Systemkomponente für Auskünfte).

Absatz 1 hält fest, dass die berechtigten Behörden ihre Auskunftsgesuche über das Verarbeitungssystem des Dienstes ÜPF einzureichen haben. Die von den Mitwirkungspflichtigen erteilten Auskünfte erhalten sie ebenfalls über das Verarbeitungssystem. Damit sind andere Übertragungswege für Auskunftsgesuche nur zulässig, wenn das Abrufverfahren mittels Verarbeitungssystem aus technischen Gründen nicht zur Verfügung steht oder in dringlichen Fällen gemäss Absatz 3. Die Auskunftsgesuche haben immer über den Dienst ÜPF zu erfolgen. Direkte Anfragen der berechtigten Behörden an die Mitwirkungspflichtigen sind nicht zulässig (s. Art. 26 Abs. 2).

Als Ausweichlösung im Falle technischer Störungen ist gemäss *Absatz 2* die Übermittlung der Auskunftsgesuche beziehungsweise der erteilten Auskünfte per Post oder Telefax vorgesehen: Auskunftsgesuche von der anfragenden Behörde an den Dienst ÜPF, erteilte Auskünfte vom Dienst ÜPF zurück an die anfragende Behörde.

Die Auskunftserteilung durch die Mitwirkungspflichtigen erfolgt ebenfalls über das Verarbeitungssystem (s. Erläuterungen zu Art. 18). Ausnahmen bestehen bei Nichtverfügbarkeit aus technischen Gründen und gemäss Artikel 18 Absatz 3 und 5 (s. Erläuterungen zu Art. 18).

In dringlichen Fällen besteht für die berechtigten Behörden die Möglichkeit, ihre Auskunftsgesuche telefonisch beim Dienst ÜPF einzureichen, mit elektronischer Nachreichung gemäss Absatz 1 oder schriftlicher Nachreichung gemäss Absatz 2 (*Abs. 3*). Diese Regelung orientiert sich an den Vorschriften für dringliche Überwachungsanordnungen gemäss Artikel 3 Absatz 1 Buchstabe c.

Absatz 4 sieht vor, dass im Auskunftsgesuch die maximale Anzahl der zu liefernden Datensätze anzugeben ist. Das Verarbeitungssystem sorgt dafür, dass

die im Auskunftsgesuch wählbare maximale Anzahl der zu liefernden Datensätze die Obergrenzen, die durch das System vorgegeben sind, nicht überschreiten kann. Dies dient zum einen als Schutzmechanismus, um nicht zu viele Ergebnisse zu bekommen, welche Kostenfolgen für die anfragende Behörde nach sich ziehen können. Zum anderen sollen sowohl das Auskunftssystem vor Überlastung geschützt als auch unspezifische Massenabfragen verhindert werden. Die Ergebnisse des Auskunftsgesuchs werden als Datensätze bezeichnet.

Art. 18 Pflichten für die Lieferung von Auskünften

In diesem Artikel werden die Pflichten der FDA und der Anbieterinnen abgeleiteter Kommunikationsdienste betreffend die Auskunftserteilung näher ausgeführt. Zuerst erscheint es notwendig zu erklären, wie die Auskunftserteilung (z. B. zum Zwecke der Teilnehmeridentifikation) üblicherweise abläuft: Die Anbieterin sucht in der Regel in den Bestandsdaten, aber auch in den aufbewahrten beziehungsweise, falls keine Überwachungspflicht besteht, in den vorhandenen Randdaten, diejenigen Angaben, auf welche die im Auskunftsgesuch angegebenen Anfragekriterien im angegebenen Zeitraum zutreffen. Sie liefert die entsprechenden Angaben über die Teilnehmenden beziehungsweise Endbenutzerinnen und -benutzer sowie über die von ihnen in Anspruch genommenen Fernmelde- beziehungsweise abgeleiteten Kommunikationsdienste nach den Vorgaben des Auskunftsgesuchs.

Aufgrund der Befreiung bestimmter FDA von Überwachungspflichten und der Verpflichtung bestimmter Anbieterinnen abgeleiteter Kommunikationsdienste zur weitergehenden Auskunftserteilung ergeben sich die folgenden Unterkategorien von Mitwirkungspflichtigen mit unterschiedlichen Pflichten betreffend die Auskunftserteilung:

- FDA, ausser jenen mit reduzierten Überwachungspflichten gemäss Artikel 51
- FDA mit reduzierten Überwachungspflichten gemäss Artikel 51
- Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten gemäss Artikel 22

Die beiden Unterkategorien von FDA haben im Prinzip die gleichen Pflichten zur Auskunftserteilung. Abweichungen für die FDA mit reduzierten Überwachungspflichten bestehen lediglich beim Verfahren der Auskunftserteilung (keine Pflicht zur Automatisierung gemäss Abs. 2 und Erlaubnis zur Auskunftserteilung ausserhalb des Verarbeitungssystems gemäss Abs. 3) sowie bei den speziellen Auskunftstypen für nicht eindeutig zugeteilte IP-Adressen (Art. 37 und 38), welche sie nicht im standardisierten Verfahren erteilen müssen, sondern formlos auf der Basis der bei ihnen vorhandenen Daten. Für alle drei der oben genannten Unterkategorien von Mitwirkungspflichtigen gilt, dass sie die Auskunftsbereitschaft herstellen müssen. Sie müssen insbesondere in der Lage sein, die Auskünfte gemäss den Vorschriften in den Artikeln 35-37 und 40-48 sowie gemäss Artikel 27 in Verbindung mit den Artikeln 35, 40, 42 und 43, die durch sie angebotene Dienste betreffen, zu erteilen (*Abs. 1*).

Die gemäss Artikel 15 BÜPF berechtigten Behörden stellen die Auskunftsgesuche mittels Verarbeitungssystem des Dienstes ÜPF (Systemkomponente für Auskünfte). Das Verarbeitungssystem vermittelt dann die Auskunftsgesuche an die

entsprechenden Mitwirkungspflichtigen, sofern diese ihre Auskünfte mittels Verarbeitungssystem erteilen. Die entsprechenden Mitwirkungspflichtigen erteilen die gewünschten Auskünfte mittels Verarbeitungssystem, das die Ergebnisse an die anfragenden Behörden weiterleitet. Bei Mitwirkungspflichtigen, die ihre Auskünfte nicht mittels Verarbeitungssystem erteilen müssen, übernimmt der Dienst ÜPF die Weiterleitung des Auskunftsgesuchs an die Mitwirkungspflichtige und er nimmt die erteilte Auskunft entgegen, um sie dann mittels Verarbeitungssystem der anfragenden Behörde zu übermitteln.

Die Auskunftstypen gemäss den Artikeln 34-41 zeichnen sich durch eine hohe Regelungsdichte aus. Die Auskunftstypen gemäss den Artikeln 34-41 entsprechen im Wesentlichen den bisherigen einfachen Auskünften A0. Aufgrund der sehr grossen Zahl von einfachen Auskünften (202'052 Auskünfte im Jahre 2016[31]) werden diese grundsätzlich über eine elektronische Schnittstelle des Verarbeitungssystems in einem automatisierten Verfahren (24 Stunden / 365 Tage) beantwortet (*Abs. 2*). Die Automatisierung erfordert genaue Vorgaben, insbesondere hinsichtlich der einzelnen Parameter und Datentypen. Diese Vorgaben sind vom EJPD in der neuen Verordnung VD-ÜPF und deren technischem Anhang 1 festgelegt.

Absatz 3 sieht vor, dass die FDA mit reduzierten Überwachungspflichten gemäss Artikel 51 die erwähnten Auskünfte auch schriftlich beantworten können, das heisst ohne die elektronische Schnittstelle des Verarbeitungssystems zu nutzen. Dies ist so vorgesehen, weil viele FDA, die zu dieser Kategorie gehören, nicht über eine solche Schnittstelle verfügen.

Es gibt spezielle Auskunftstypen für nicht eindeutig zugeteilte IP-Adressen (Art. 38 und 39) und weitere Auskunftstypen (Art. 42-47), die auch mittels manueller Verfahren erteilt werden können. Bei diesen steht es den Mitwirkungspflichtigen frei, die Auskünfte manuell oder automatisiert zu erteilen. Die Mitwirkungspflichtigen, die ihre Auskünfte mittels Verarbeitungssystem erteilen müssen (*Abs. 4*), müssen jedoch auch die manuelle Erteilung von Auskünften über das Verarbeitungssystem vornehmen (*Abs. 2*).

Absatz 4 regelt die Pflichten für die Erteilung der Auskunftstypen nach Artikel 38 (IR_8_IP (NAT)) und Artikel 39 (IR_9_NAT), welche die Aufbewahrung von Randdaten während 6 Monaten erfordern. Die FDA mit reduzierten Überwachungspflichten (Art. 51) sind von der Pflicht zur Randdatenaufbewahrung befreit. Daher sind sie von der Erteilung der standardisierten Auskunftstypen nach Artikel 38 und 39 ebenfalls ausgenommen. Sie sind jedoch nicht von der formlosen Auskunftserteilung basierend auf vorhandenen Randdaten befreit.

In *Absatz 5* wird präzisiert, welche Kategorien von Mitwirkungspflichtigen nicht verpflichtet sind, die Auskünfte gemäss den definierten Auskunftstypen zu erteilen. Sie liefern die ihnen vorliegenden Angaben schriftlich per Post oder Telefax oder mit einem durch den Dienst ÜPF zugelassenen sicheren Übertragungsmittel. Es handelt sich um die Anbieterinnen abgeleiteter Kommunikationsdienste ohne weitergehende Auskunftspflichten (diejenigen, die die in Art. 22 festgelegten Voraussetzungen nicht erfüllen) und die Betreiberinnen interner Fernmeldenetze (Art. 1 Abs. 2 Bst. k). Die beiden vorgenannten Kategorien von Mitwirkungspflichtigen können freiwillig ihre Auskünfte gemäss dem standardisierten

31 Statistik des Dienstes ÜPF: www.li.admin.ch/de/themen/statistik

Verfahren über das Verarbeitungssystem erteilen. Von der eingangs genannten Pflicht ausgenommen sind auch Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen (Art. 1 Abs. 2 Bst. l). Sie müssen jedoch im Falle einer angeordneten Überwachung die für die Überwachung notwendigen Auskünfte erteilen (Art. 29 Abs. 1 Bst. b BÜPF).

Falls die Anzahl der gefundenen Ergebnisse die im Auskunftsgesuch angegebene maximale Anzahl der zu liefernden Datensätze überschreitet, liefert die Anbieterin nur eine entsprechende Meldung mit der Anzahl der gefundenen Ergebnisse, aber keine Daten (*Abs. 6*). Die anfragende Behörde kann dann das Auskunftsgesuch neu stellen mit verfeinerten Anfragekriterien und/oder mit einem höheren Wert der Höchstzahl der zu liefernden Datensätze, sofern die durch das Auskunftssystem vorgegebene Obergrenze nicht überschritten wird. Falls die anfragende Behörde mehr Ergebnisdatensätze benötigt, als es die Obergrenzen des Verarbeitungssystems zulassen, kann sie das Auskunftsgesuch als besondere Auskunft im Sinne des Artikel 25 an den Dienst ÜPF stellen.

Art. 19 Identifikation der Teilnehmenden

Grundsätzlich genügt es, wenn die FDA, die den entsprechenden Fernmeldedienst erbringt, die Teilnehmenden mit geeigneten Mitteln identifiziert (*Abs. 1*).

Bei professionell betriebenen öffentlichen WLAN-Zugangspunkten müssen die FDA jedoch die Identifikation der Endbenutzenden, also der tatsächlichen Benutzer, mit geeigneten Mitteln sicherstellen (*Abs. 2*). Mit "professionell betrieben" ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen. Hier genügt die Identifikation des Teilnehmenden gemäss Absatz 1. Die Einschränkung auf "professionellen Betrieb" erfolgt aus Gründen der Verhältnismässigkeit, damit beispielsweise Privathaushalte und Kleinbetriebe, die ihr WLAN "offen" lassen, nicht von der aufwendigeren Identifikation der Endbenutzenden betroffen sind.

Unter geeigneten Mitteln der Identifikation, auch mittelbare Identifikation genannt, sind implizite oder vereinfachte Registrierungen mittels vertrauenswürdiger (trusted) Angaben zu verstehen. Denkbare Beispiele sind:

- Zugangscode per SMS an Mobiltelefon und Speicherung der MSISDN;
- Identifikation mittels Kreditkarte und Speicherung der Autorisierungsdaten;
- Identifikation mittels gültiger Bordkarte auf Flughäfen und Speicherung der Bordkartendaten;
- Identifikation mittels Karte eines Vielfliegerprogramms, die den Zugang zur Lounge ermöglicht, und Speicherung der Autorisierungsdaten;
- Identifikation mittels maschinenlesbarer Zeile (MRZ) des Identitätsdokuments und Speicherung der MRZ-Daten;

- Identifikation mittels vertrauenswürdiger Angaben von Roaming-Partnern und Speicherung der Autorisierungsdaten;
- individueller Zugangscode im Hotel, der an eine Gastregistrierung gekoppelt ist;
- Identifikation über SIM-Karte und Speicherung der IMSI.

Art. 20 Erfassung von Angaben zur Person bei Mobilfunkdiensten

Artikel 20 entspricht unter anderem dem Artikel 19*a* der VÜPF vom 31. Oktober 2001[32] und bringt die nötigen Präzisierungen an. Er stützt sich dabei namentlich auf die Delegationsnormen an den Bundesrat in Artikel 21 Absatz 1 Buchstabe d, Artikel 22 Absatz 2 und Artikel 23 Absatz 1 BÜPF[33].

Absatz 1 sieht vor, dass bei der erstmaligen Aktivierung von Zugangsmitteln zu Mobilfunkdiensten (z. B. GSM, GPRS, UMTS, LTE, VoLTE, VoWiFi) die Teilnehmenden anhand eines Reisepasses, einer Identitätskarte oder eines Ausländerausweises im Sinne der Artikel 71 und 71a der Verordnung vom 24. Oktober 2007 über Zulassung, Aufenthalt und Erwerbstätigkeit (VZAE) zu identifizieren sind. Unter "Aktivierung" ist der Zeitpunkt zu verstehen, ab dem ein Teilnehmender den entsprechenden Dienst nutzen kann, z. B. bei bereits aktivierten Zugangsmitteln der Zeitpunkt von deren Abgabe oder bei einer Embedded SIM (eSIM), welche fest im Gerät eingebaut ist, die Aktivierung des entsprechenden Profils durch die Anbieterin. Beispiel: Ein für Mobilfunk vorbereitetes Tablet mit fest eingebauter SIM-Karte (eSIM) wird von einem Elektronikgeschäft, welches nicht selbst die Aktivierung eines Mobilfunkdienstes vornehmen kann, an einen Kunden verkauft. Der Kunde kann das Tablet zunächst nur über WiFi benutzen. Erst wenn er von einer Mobilfunkanbieterin die eSIM aktivieren lässt, kann er das « Zugangsmittel » (die im Tablet eingebaute eSIM) 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, als es aktiviert wurde. Ausserdem ist ebenfalls wichtig, wer die Registrierung durchführen muss. Das Elektronikgeschäft führt in diesem Beispiel die Aktivierung des Zugangsmittels zum Mobilfunk nicht durch. Daher muss das Elektronikgeschäft hier nicht registrieren (d. h. es gilt nicht als Wiederverkäuferin von Karten und ähnlichen Mitteln), sondern dies ist Aufgabe der Mobilfunkanbieterin bei der Aktivierung der eSIM.

Bei erneuten Kundenkontakten gehen wir davon aus, dass die Anbieterinnen immer auch die Angaben und den Ausweis prüfen, weil sie ein eigenes Interesse daran haben. Der Begriff *Zugangsmittel* ist die Kurzform von "das für den Zugang zum Fernmeldedienst erforderliche Mittel" (Art. 21 Abs. 1 Bst. e BÜPF).

Bei Mobilfunkdiensten ist die Überprüfung der Identität des Kunden anhand eines Ausweises zwingend. Dies entspricht der bisherigen Regelung für vorbezahlte Mobilfunkdienste (Prepaid), welche neu auf alle Mobilfunkdienste unabhängig von der Zahlungsmethode (z. B. Abonnement, vorbezahlt, gratis) ausgedehnt wird. In der Praxis verlangen die Mobilfunkanbieterinnen beim Abschluss von Abonnementen bereits seit langem die Vorlage eines Ausweisdokuments.

32 SR **780.11**
33 Siehe Botschaft zum BÜPF vom 27. Februar 2013, BBl **2013** 2734.

Die Anbieterinnen von Fernmeldediensten, die Anbieterinnen von abgeleiteten Kommunikationsdiensten mit weitergehenden Auskunftspflichten gemäss Artikel 22 und die Wiederverkäuferinnen gemäss Artikel 2 Buchstabe f BÜPF müssen dafür sorgen, dass die Erfassung der Angaben zur Person korrekt anhand des vorgelegten Ausweises erfolgt (Art. 23 Abs. 1 BÜPF). Zur Kontrolle dient die Ausweiskopie. Falls der 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 (YYMMDD);
- Geschlecht ("M"=männlich / "F"=weiblich / "<"=keine Angabe).

Hinweis: In dieser Verordnung bedeutet die Formulierung "falls vorhanden" (if available), dass die entsprechenden Daten zu liefern sind, wenn sie technisch vorhanden sind, zum Beispiel ein bestimmter Parameter in einer Signalisierungsmeldung. Im Einzelnen hängt das von einer Vielzahl von Faktoren ab, wie der Technologie, den anwendbaren Standards, dem Kommunikationsdienst und dem konkreten Szenario. Die Einzelheiten sind im Anhang 1 der VD-ÜPF geregelt. Es besteht also eine Pflicht für die Anbieterinnen, wenn die Daten existieren, diese auch zu liefern beziehungsweise für die Zwecke von Auskünften und rückwirkenden Überwachungen zu speichern. Beispiel: Eine Kundennummer existiert nicht immer und es muss auch keine von der Anbieterin generiert werden. Daher steht bei Artikel34 Absatz 1 Buchstabe a "falls vorhanden". Die Formulierung "falls vorhanden" darf nicht mit der Formulierung "die ihnen zur Verfügung stehenden Randdaten" im BÜPF verwechselt werden (z. B. in Art. 28 Abs. 2 BÜPF), welche eine passive Duldungspflicht ausdrückt und keine aktive Speicherpflicht.

Angaben gemäss Absatz 2 beziehungsweise 3, die nicht im Ausweis stehen (z. B. Adresse), sind gemäss den Kundenangaben zu erfassen und entsprechend zu liefern. Die bei der Registrierung erfassten Angaben und die elektronische Ausweiskopie sind von der Wiederverkäuferin an die Anbieterin weiterzuleiten, zu deren Diensten das wiederverkaufte Mittel den Zugang ermöglicht.

Wenn der Kunde beziehungsweise die Kundin oder die Anbieterin Angaben ändern (z. B. neue Rechnungsadresse) sind diese ebenfalls zu speichern, es besteht jedoch keine Pflicht zur fortlaufenden Überprüfung und Aktualisierung dieser Daten. So wird insbesondere auch keine Nachregistrierung von Angaben zum Kunden verlangt. Angemerkt sei, dass die Anbieterin bei einer falsch registrierten

Kundenbeziehung ohne Abonnementsverhältnis (Prepaid) den betreffenden Zugang zu Fernmeldediensten sperren muss (Art. 6*a* FMG[34]).

Wichtig ist, dass die bei der Registrierung erfassten Daten während der gesamten Dauer der Kundenbeziehung sowie während 6 Monaten nach deren Beendigung durch die Anbieterin aufbewahrt werden müssen (Art. 21 Abs. 2 BÜPF).

Weitere Massnahmen wurden notwendig, weil in der Vergangenheit viele Falschregistrierungen von Teilnehmerdaten stattgefunden haben. Die Ausweiskopie erscheint zurzeit als das geeignetste Mittel, um solchen Falschregistrierungen vorzubeugen. Andere Lösungsansätze wurden bisher keine genannt. Es sind allenfalls weitere Möglichkeiten wie Swiss-ID, elektronische Identität (eID) oder ähnliches denkbar (s. Bundesgesetz vom 19. Dezember 2003[35] über Zertifizierungsdienste im Bereich der elektronischen Signatur [Bundesgesetz über die elektronische Signatur, **ZertES**] und zukünftiges eID-Gesetz[36]) (s. Art. 23 Abs. 1 BÜPF). Auch eine Online Identifizierung, welche den Sicherheits- und Qualitätsstandards nach dem FINMA-Rundschreiben 2016/7 «Video- und Online-Identifizierung» für den Bankenbereich entspricht, wäre denkbar. Bei der Identifizierung des Teilnehmenden anhand einer gültigen elektronischen Identität (eID) oder ähnlichem, bei der vorgenannten Online Identifizierung und bei gleichwertigen Verfahren kann auf das persönliche Erscheinen des Teilnehmenden verzichtet werden.

Der Ausweis muss nicht unbedingt in Papierform kopiert und aufbewahrt werden. Es muss aber eine gut lesbare elektronische Ausweiskopie im System der Anbieterin vorhanden sein (Abs. 1, 2. Satz), egal ob es sich hier um eine Fotografie oder einen Scan handelt (s. Art. 23 Abs. 1 BÜPF). Bei der Identifizierung des Teilnehmenden anhand einer elektronischen Identität oder ähnlichem sind die Angaben elektronisch zu erfassen und die Ausweiskopie entfällt. Angaben gemäss Absatz 2 beziehungsweise 3, die nicht in der elektronischen Identität enthalten sind (z. B. Adresse), sind gemäss den Angaben des Teilnehmenden zu erfassen.

Absatz 2 präzisiert die Angaben, die bei natürlichen Personen zu erfassen sind. Die benötigten Angaben (Name[n], Vorname [n], Geburtsdatum, Art des Ausweises, Ausweisnummer, Adresse) waren schon im Artikel 19*a* der VÜPF vom 31. Oktober 2001[37] vorgesehen und entsprechen der bisherigen Praxis. Neu sind auch das ausstellende Land beziehungsweise die ausstellende Organisation, die Nationalität (Art. 21 Abs. 1 Bst. d BÜPF) und falls bekannt der Beruf anzugeben (Art. 21 Abs. 1 Bst. a BÜPF). Die Angabe des Landes beziehungsweise der Organisation, das beziehungsweise die den Ausweis ausgestellt hat, ist für die Strafverfolgungsbehörden notwendig, um allfällige Überprüfungen vornehmen zu können.

Absatz 3 regelt, welche Angaben bei den juristischen Personen zu erfassen sind. Die neu zu erfassenden Angaben sind der Name, der Sitz und die Kontaktdaten der juristischen Person (*Bst. a*), die Unternehmens-Identifikationsnummer (UID) gemäss dem Bundesgesetz vom 18. Juni 2010[38] über die Unternehmens-

34 BBl **2016** 2019
35 SR **943.03**
36 https://www.egovernment.ch/de/umsetzung/schwerpunktplan/elektronische-identitat/
37 SR **780.11**
38 SR **431.03**

Identifikationsnummer (*Bst. b*) sowie falls vorhanden, die Namen und Vornamen der Personen, welche die Dienste der Anbieterin in Anspruch nehmen, zum Beispiel die Mitarbeitenden (*Bst. c*).

Absatz 4 verpflichtet die FDA, die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten und die Wiederverkäuferinnen, bei Kundenbeziehungen ohne Abonnementsverhältnis (Prepaid, Gratisangebote) weitere Angaben zu erfassen. Nicht betroffen sind die einfachen Telefonkarten, die anstelle von Geld zum Telefonieren in den Telefonkabinen verwendet werden können (z. B. die in den Kiosken verkauften, mit Guthaben geladenen "Taxcards")[39]. Gemäss Artikel 1 Buchstabe b der Verordnung vom 9. März 2007[40] über Fernmeldedienste (FDV) ist ein Kunde eine natürliche oder juristische Person, die mit einer Anbieterin von Fernmeldediensten einen Vertrag über die Inanspruchnahme von deren Diensten geschlossen hat. Dies gilt analog auch für Kunden von abgeleiteten Kommunikationsdiensten. Der Grund für die Erfassung dieser weiteren Angaben liegt darin, dass nachvollziehbar sein muss, wer allfällige Falschregistrierungen vorgenommen hat (s. a. entsprechende Strafbestimmung in Art. 39 Abs. 1 Bst. c BÜPF).

Art. 21 Aufbewahrungsfristen

Artikel 21 stellt die Ausführungsbestimmung des Artikels 21 Absatz 2 (Auskünfte über Fernmeldedienste) und des Artikels 22 Absatz 2 BÜPF (Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet) dar.

Absatz 1 1. Satz sieht vor, dass alle Angaben über die Fernmeldedienste und jene zur Identifikation der Täterschaft bei Straftaten über das Internet grundsätzlich während der Dauer der Kundenbeziehung sowie während 6 Monate nach deren Beendigung aufzubewahren und elektronisch zu liefern sind. Zu den *Angaben über die Fernmeldedienste* gehören auch die Angaben zur Person gemäss Artikel 20 Absätze 1-3. Ausserdem sei hier auch auf die Übergangsbestimmung in Artikel 45 Absatz 3 BÜPF verwiesen.

Absatz 1 2. Satz regelt, analog zum 1. Satz, die Aufbewahrungsdauer für Identifikationsdaten gemäss Artikel 19 Absatz 2, welche die FDA bei professionell betriebenen öffentlichen WLAN-Zugangspunkten erfassen müssen. Um die Benutzerverwaltung an professionell betriebenen öffentlichen WLAN-Zugangspunkten zu vereinfachen, wird als Äquivalent zur Dauer der Kundenbeziehung die Dauer der Zugangsberechtigung zum öffentlichen WLAN-Zugangspunkt verwendet.

In Ausführung von Artikel 21 Absatz 2 zweiter Satz und Artikel 22 Absatz 2 zweiter Satz BÜPF bestimmt *Absatz 2* die Angaben, die nur während 6 Monaten aufzubewahren und zu liefern sind, damit kein Widerspruch zur Aufbewahrungsfrist gemäss Artikel 26 Absatz 5 BÜPF besteht. Diese Aufbewahrungsfrist ist eine kürzere Frist als die von Absatz 1. Diese Angaben sind die Liste der tatsächlich benutzten Geräteidentifikatoren, zum Beispiel IMEI, MAC-Adresse (s. Art. 36 Abs. 1 Bst. d und 41 Abs. 1 Bst. d), sowie die Angaben zur Erteilung der Auskünfte gemäss den Artikeln 37, 38 und 39.

39 Siehe Botschaft zum BÜPF vom 27. Februar 2013, BBl **2013** 2709.
40 SR **784.101.1**

Für die FDA mit reduzierten Überwachungspflichten gemäss Artikel 51 wäre die Aufbewahrungspflicht gemäss Absatz 2 ein Widerspruch zu der mit Artikel 51 beabsichtigten Befreiung von den Überwachungspflichten. Diese Befreiung wird daher auch hier konsequent umgesetzt.

Mit *Absatz 3* wird der Empfehlung der Kommission für Rechtsfragen des Nationalrates vom 19. September 2017 entsprochen, dass aus Gründen der Rechtssicherheit für die in Absatz 2 genannten Daten eine Löschpflicht nach 6 Monaten vorzusehen sei.

Art. 22 Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten

Abgeleitete Kommunikationsdienste werden immer mehr eingesetzt und nehmen entsprechend immer mehr an Bedeutung zu. Die gewöhnlichen Anbieterinnen abgeleiteter Kommunikationsdienste haben im Bereich der Fernmeldeüberwachung aufgrund der gesetzlichen Vorgaben weniger weitreichende Pflichten als die gewöhnliche FDA (nicht reduzierte). Sie haben eine Überwachung lediglich zu dulden und die ihnen vorliegenden Angaben herauszugeben, die für die Durchführung der Fernmeldeüberwachung notwendig sind. Dazu haben sie, die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person auf Verlangen zu liefern (Art. 27 Abs. 2 BÜPF). Wenn eine Straftat über das Internet begangen wird, kann es jedoch vorkommen, dass diese Minimalpflicht nicht ausreicht. Aus diesem Grund hat der Gesetzgeber in Artikel 22 Absatz 4 BÜPF dem Bundesrat die Kompetenz eingeräumt, auch den Anbieterinnen abgeleiteter Kommunikationsdienste weitergehende Auskunftspflichten aufzuerlegen. Bei den zu erfüllenden Pflichten handelt es sich um dieselben Pflichten, die von den FDA zu erfüllen sind. Die Anbieterinnen abgeleiteter Kommunikationsdienste, die weitergehende Pflichten haben, müssen somit allen Pflichten gemäss Artikel 22 Absatz 1 und 2 BÜPF nachkommen.

Absatz 1 konkretisiert die einzelnen Voraussetzungen, welche erfüllt sein müssen, damit eine Anbieterin abgeleiteter Kommunikationsdienste weitergehende Auskunftspflichten hat. Eine Anbieterin hat dann weitergehende Auskunftspflichten, wenn sie gemäss *Buchstabe a* 100 Auskunftsgesuche in den letzten zwölf Monaten auszuführen hatte (wobei der 30. Juni als Stichtag dient) oder gemäss *Buchstabe b* einen Jahresumsatz in der Schweiz von 100 Millionen Franken in zwei aufeinander folgenden Geschäftsjahren erzielt.

Buchstabe a nimmt das in Artikel 22 Absatz 4 BÜPF genannte Kriterium „grosse Benutzerschaft“ auf. Aus Sicht der Fernmeldeüberwachung ist es sehr schwierig, die grosse Benutzerschaft *absolut* zu definieren, umso mehr, wenn es gilt, diese in Bezug auf verschiedene angebotene technische Dienste im Voraus festzulegen. Aus diesem Grund wird mit Buchstabe a ein praxiserprobtes Kriterium angewandt, nämlich jenes der Anzahl Auskunftsgesuche. Die Statistik der Fernmelde-überwachungen der letzten Jahre zeigt, dass die Anzahl Auskunftsgesuche verlässlich und passend auf die Art der angebotenen Dienste zuverlässig die grosse Benutzerschaft erfasst. Gleichzeitig wird mit diesem Kriterium auch die Verhältnismässigkeit abgedeckt, indem nur Anbieterinnen erfasst werden, die auch wirklich relevant für die Fernmeldeüberwachung sind.

Das zweite Kriterium, *Buchstabe b*, wird dadurch weiter eingeschränkt, dass nur solche Anbieterinnen in die Pflicht gezogen werden, bei denen ein grosser Teil ihrer Geschäftstätigkeit im Anbieten von abgeleiteten Kommunikationsdiensten besteht und ihre Dienste zudem von mindestens 5000 Teilnehmenden in Anspruch genommen werden. Weil die Schwellenwerte zum Schutz der Schweizer KMU sehr hoch angesetzt sind, werden zahlenmässig relativ wenigen Anbieterinnen abgeleiteter Kommunikationsdienste weitergehende Auskunftspflichten auferlegt.

Absatz 2 bildet den sogenannten Konzerntatbestand. Kontrolliert eine Anbieterin eine oder mehrere rechnungspflichtige Unternehmen, werden sie bei der Berechnung der Grössen gemäss Absatz 1 Buchstaben a und b als eine Einheit betrachtet. Es wird dabei auf die Regelung von Artikel 963 Absatz 1 und 2

Obligationenrecht (OR) verwiesen, welche sinngemäss Anwendung findet. Zu erwähnen ist, dass die Muttergesellschaft und das kontrollierte Unternehmen nur in Bezug auf die von ihnen angebotenen Kommunikationsdienste als eine Einheit behandelt werden.

Absatz 3 sieht für die Anbieterinnen eine Meldepflicht vor für den Fall, dass sie die Schwellenwerte gemäss Absatz 1 Buchstaben a oder b unter- oder überschreitet. Dafür stellt der Dienst ÜPF geeignete Meldemechanismen zur Verfügung.

Absatz 4 gibt dem Dienst ÜPF die notwendigen Mittel, um nachzuvollziehen, ob vor allem die in Absatz 1 genannten Grössen tatsächlich über- oder unterschritten wurden. Allerdings benötigt der Dienst ÜPF auch Daten um festzustellen, ob eine Anbieterin als eine mit abgeleiteten Kommunikationsdiensten gilt oder nicht. Dazu kann er auch benötigte Unterlagen von anderen Behörden einholen, wie Steuerunterlagen.

Absatz 5 sieht vor, dass eine Anbieterin, welche die Voraussetzungen gemäss Absatz 1 erfüllt, innert zwei Monaten die für die Auskunftserteilung erforderlichen Daten speichern und innert zwölf Monaten auskunftsbereit sein muss. Die Frist beginnt ab Kenntnisnahme des Entscheides des Dienstes ÜPF zu laufen. Der Dienst ÜPF unterstützt die Anbieterin beratend bei der Erfüllung ihrer Pflichten.

Art. 23 Erfüllungsgehilfen zur Erteilung von Auskünften und Durchführung von Überwachungen

Artikel 23 regelt den Beizug von Erfüllungsgehilfen durch die Anbieterinnen. Es ist wesentlich, dass durch deren Beizug weder Verzögerungen noch Qualitätsverluste oder gar Überwachungslücken entstehen. Deshalb unterstehen die Erfüllungsgehilfen denselben Vorgaben wie die Anbieterinnen. Zudem soll der Dienst ÜPF bei Notwendigkeit, unter anderem wenn ein Problem mit der Ausleitung besteht, direkt die Anbieterin oder den Erfüllungsgehilfen kontaktieren können, je nachdem welche Vorgehensweise der Dienst ÜPF im Einzelfall als zielführender ansieht.

Art. 24 Standardisierung von Auskunfts- und Überwachungstypen

In diesem Artikel geht es um die technische und administrative Standardisierung der in dieser Verordnung definierten Auskunfts- und Überwachungstypen.

Unter Standardisierung eines Auskunfts- oder Überwachungstyps durch das EJPD (*Abs. 1*) versteht man die Regelung von dessen technischen und administrativen Einzelheiten in der Verordnung des EJPD VD-ÜPF (zum Begriff Auskunftstyp, s. die Erläuterungen zu Art. 26; zum Begriff Überwachungstyp, s. die Erläuterungen zu Art. 28). Die Voraussetzungen für diese Standardisierung sind zum einen die Existenz der entsprechenden internationalen Standards und zum anderen die Machbarkeit und Verhältnismässigkeit ihrer Umsetzung in der Praxis.

Sollten diese Voraussetzungen für bestimmte Typen bei Inkraftsetzung dieser Verordnung noch nicht gegeben sein, verzichtet das EJPD nach *Absatz 2* vorerst auf deren Standardisierung.

Gemäss Artikel 31 Absatz 3 BÜPF soll das EJPD selber bestimmen können, welches die «gängigen», das heisst für eine Standardisierung geeigneten Typen sind. Die vom Bundesrat definierten und die vom EJPD standardisierten Typen

sollen nicht streng aneinander gebunden sein, damit dem EJPD in eigener Verantwortung der Spielraum für eine Erweiterung, Reduktion oder Verschiebung des Kreises der standardisierten Typen bleibt und es dafür nicht immer gleichzeitig eine Revision der Bundesratsverordnung VÜPF erwirken muss.

Art. 25 Besondere Auskünfte und Überwachungen

Alle gängigen Auskunfts- und Überwachungstypen sind in den Artikeln 24 und 25 erwähnt und in den 1. (Art. 27) und 4.-6. (Art. 35-48) beziehungsweise 8.-11. Abschnitten (Art. 54-68) des 3. Kapitels geregelt.

Die nicht explizit in dieser Verordnung aufgeführten Auskünfte und Überwachungen stellen sogenannte Spezialmassnahmen dar. Diese werden vom Dienst ÜPF oder durch von diesem beauftragte Personen durchgeführt. Dies entspricht der bisherigen Praxis gemäss Artikel 17 Absatz 5 und Artikel 25 Absatz 5 VÜPF vom 31. Oktober 2001[41]. Diese Bestimmungen wurden mit der Änderung vom 23. November 2011 (in Kraft seit dem 1. Januar 2012) eingefügt, um die Befugnis des Dienstes ÜPF, die Durchführung von Überwachungsmassnahmen, die nicht explizit in der VÜPF aufgeführt sind, die aber durch die Strafverfolgungsbehörden angeordnet und von den Zwangsmassnahmengerichten genehmigt wurden, gegenüber den betroffenen Anbieterinnen verfügen zu können, gesondert zu regeln. Gemäss dem Entscheid des Bundesverwaltungsgerichts vom 23. Juni 2011 (A-8267/2010) müssen die betroffenen Anbieterinnen die Durchführung solcher Überwachungsmassnahmen dulden. Sie müssen dem Dienst ÜPF die Schnittstellen zur Verfügung stellen, die bereits vorhanden sind..

Zu den Duldungspflichten der Anbieterin zählt auch der Zugang zu den Anlagen (Art. 52), insbesondere die kostenlose Zurverfügungstellung bestehender Netzzugänge zu öffentlichen Fernmeldenetzten.

Art. 26 Auskunftstypen im Allgemeinen

Absatz 1 dient als Kurzübersicht über die verschiedenen Auskunftstypen, welche in den Abschnitten 1 und 4-6 des 3. Kapitels (Art. 27 und 34-47) definiert werden. Unter einem Auskunftstyp versteht man eine in dieser Verordnung näher bestimmte Art und Weise des Gesuchs und der Erteilung von Auskünften über die Daten gemäss den Artikeln 21 und 22 BÜPF im Zusammenhang mit Fernmeldediensten oder abgeleiteten Kommunikationsdiensten.

Neu sind die Auskunftstypen gemäss ETSI-Norm TS 102 657 organisiert. Die Auskunftstypen sind nach Dienstkategorien unterteilt. Diese Unterteilung ist durch die ETSI-Norm vorgegeben. Da die Produkte der Anbieterinnen mehrere Dienstkategorien umfassen können (z. B. Mobilfunkabonnement mit den Dienstkategorien Netzzugang sowie Telefonie- und Multimediadienste) sollte in der Praxis je ein Auskunftsgesuch pro Auskunftstyp eingeholt werden, um alle Dienste abzufragen.

Für die am häufigsten unter den Auskunftsgesuchen vertretenen Dienstkategorien *Netzzugangsdienste* sowie *Telefonie- und Multimediadienste* gibt es eine Unterteilung in die Typen "Auskünfte über Teilnehmende" (Art. 35 und 40) und die Typen "Auskünfte über Dienste" (Art. 36 und 41). Diese Aufteilung entspricht

41 SR **780.11**

in etwa den bisherigen Auskünften A0 und A1 und dient dazu, den Umfang der Informationen pro Auskunftstyp zu begrenzen, um die automatisierte Bearbeitung zu erleichtern und zu beschleunigen.

Bei den weniger häufig angefragten Dienstkategorien *E-Mail-Dienste* sowie *andere Fernmelde- oder abgeleitete Kommunikationsdienste* wurde auf diese Unterteilung verzichtet.

Bei der Dienstkategorie *Netzzugangsdienste* kommen noch drei spezifische Auskunftstypen (Art. 36-38) für die Zwecke der Identifikation der Benutzerschaft bei Straftaten über das Internet (Art. 22 BÜPF) hinzu.

Bei den Auskunftstypen gemäss den Artikeln 35, 40, 42 und 43 ist jeweils eine flexible Namenssuche möglich, die in Artikel 27 definiert wird.

Gemäss *Absatz 2* dürfen Informationen, über welche die Anbieterinnen im Rahmen dieser Verordnung Auskunft erteilen müssen, von den Behörden auch nur in dem in dieser Verordnung vorgesehenen Verfahren angefragt werden, das heisst die Behörden stellen ihre Auskunftsgesuche mittels Verarbeitungssystem des Dienstes ÜPF oder, unter den Voraussetzungen des Artikels 17 Absätze 2 und 3, an den Dienst ÜPF per Post oder Telefax beziehungsweise telefonisch, aber nie direkt an die Mitwirkungspflichtigen.

Art. 27 Auskunftstypen mit flexibler Namenssuche

In diesem Artikel werden vier zusätzliche Auskunftstypen zusammengefasst, die auf den Auskunftstypen gemäss den Artikeln 35 (IR_4_NA), 40 (IR_10_TEL), 42 (IR_13_EMAIL) und 43 (IR_15_COM) basieren und sich von diesen nur in der Art der Namenssuche unterscheiden:

- IR_5_NA_FLEX;
- IR_11_TEL_FLEX;
- IR_14_EMAIL_FLEX;
- IR_16_COM_FLEX.

Die Namenssuche ist das Anfragekriterium gemäss dem jeweiligen Absatz 2 Buchstabe a der vorgenannten Artikel. Es handelt sich um eine phonetische und fehlertolerante (kurz: flexible) Namenssuche. Da die ETSI-Schnittstelle für Auskunftsgesuche und -antworten nicht die Möglichkeit der Übermittlung von Anweisungen über die Art der Suche zulässt, wurden diese vier zusätzlichen Auskunftstypen definiert.

Auskunftsgesuche nach Namen werden künftig automatisiert von den FDA und den Anbieterinnen abgeleiteter Kommunikationsdienste mit erweiterten Auskunftspflichten ausgeführt. Diese Suchen wurden bisher von Mitarbeitenden der Anbieterinnen durchgeführt, wobei deren menschliche Intelligenz zum Tragen kam. Um künftig bei der automatisierten Namenssuche mindestens gleichwertige Ergebnisse zu erzielen, muss neben der buchstabengetreuen Suche (Basistypen gemäss Art. 35, 40, 42 und 43) auch die Möglichkeit einer fehlertoleranten und phonetischen Suche bestehen. Damit wird den Bedürfnissen der Strafverfolgungsbehörden Rechnung getragen.

In der Praxis hat sich nämlich gezeigt, dass die Erfassung der Personendaten häufig wie folgt fehlerbehaftet ist:

1. Fehlende oder in der Reihenfolge vertauschte Namensteile
2. Schreibfehler
3. Unterschiedliche Transliteration von Namen aus ausländischen Alphabeten in unterschiedliche lateinische Zeichensätze. Dies kann bereits im Ausweisdokument passiert sein. Häufig geschieht es jedoch bei der Registrierung, das heisst bei der Erfassung der Personendaten oder bei der Speicherung der Daten in der Kundendatenbank, da IT-Systeme häufig nicht alle existierenden diakritischen Zeichen unterstützen.
4. Unterschiedliche Transkription (z. B. englisch, französisch) von Namen aus nicht-lateinischer Schrift in lateinische Schrift

Bei der flexiblen Namenssuche ist daher kein exakter Vergleich der Zeichenketten durchzuführen, sondern einerseits eine Suche nach phonetischer Übereinstimmung und andererseits ein Abgleich der Namensbetandteile (name matching), um beispielsweise auch Übereinstimmungen von Namensteilen und deren Reihenfolgevertauschungen zu erkennen. Gängige Datenbankmanagementsysteme enthalten bereits auf die flexible Namenssuche spezialisierte Suchfunktionen. Für weitere Einzelheiten zur flexiblen Suche sei auf die Erläuterungen zu Artikel 13 Absatz 2 VD-ÜPF verwiesen.

Art. 28 Überwachungstypen

Dieser Artikel dient als Kurzübersicht über die verschiedenen Überwachungstypen, die in den Abschnitten 8 bis 11 des 3. Kapitels (Art. 54-68) definiert werden. Unter einem Überwachungstyp versteht man eine in dieser Verordnung näher bestimmte Art und Weise der Überwachung eines oder mehrerer Fernmeldedienste beziehungsweise abgeleiteter Kommunikationsdienste (Art. 31 Abs. 1 BÜPF). Unterschieden wird zwischen Echtzeitüberwachungen (Abs. 1), rückwirkenden Überwachungen (Abs. 2) sowie Notsuchen (Abs. 3) und Fahndungen (Abs. 4).

Die Überwachungstypen der Echtzeitüberwachung sind so aufgebaut, dass die Strafverfolgungsbehörden bei den wichtigsten Dienstkategorien neu die Möglichkeit haben, entweder nur die Lieferung in Echtzeit der Randdaten oder die Lieferung in Echtzeit der Inhalts- und Randdaten zu verlangen (Abs. 1). Dadurch soll eine Möglichkeit geschaffen werden, die Schwere des Grundrechtseingriffs abstufen zu können.

Inhaltsdaten (z. B. Gespräche, E-Mail-Texte und Anhänge) können nur im Rahmen einer Echtzeitüberwachung beschafft werden. Bei rückwirkenden Überwachungen (Randdaten der rückwirkenden Überwachung, auch Randdaten des vergangenen Fernmeldeverkehrs oder Vorratsdaten genannt) werden hingegen Inhaltsdaten nicht gespeichert (zum Begriff Randdaten, s. auch die einleitenden Erläuterungen zum 10. Abschnitt des 3. Kapitels).

Die Überwachung des Fernmeldeverkehrs ist so aufgebaut, dass für die wichtigsten Dienstkategorien eigenständige Überwachungstypen definiert sind. Dadurch wird einerseits dem Bestimmtheitsgebot Rechnung getragen und anderseits den Vorgaben der internationalen Standards entsprochen. Die Dienstkategorien werden unterteilt in Netzzugangsdienste und Anwendungen (engl.: application). Zu den Anwendungen gehören dabei die Telefonie- und Multimediadienste, die E-Mail-Dienste sowie andere Fernmelde- und abgeleitete Kommunikationsdienste.

Traditionell waren bei der Telefonie Netzzugang und Anwendung identisch (Telefonanschluss). Somit genügte es in der Regel, den Anschluss zu überwachen. Im Zuge des technischen Fortschritts gibt es jedoch immer mehr Kommunikationsdienste, bei denen der Netzzugang fast beliebig sein kann. Eine Überwachung am Netzzugang (Anschluss) wäre bei solchen Diensten wenig erfolgversprechend. Dies umso mehr, wenn die Kommunikation zudem noch von der Anbieterin oder den Endgeräten beziehungsweise Clients verschlüsselt wird. Dies wird am Beispiel der nomadischen Internettelefonie (VoIP) deutlich: Die Zugangsdaten des Teilnehmenden können beispielsweise in einer App auf dem Smartphone gespeichert sein. Der Teilnehmende kann das Smartphone an einem beliebigen Internetzugang verwenden (z. B. im Hotel, im Büro, am Flughafen) und kann mit Hilfe der App die Internet-Telefoniedienste in Anspruch nehmen. Da die Strafverfolgungsbehörden zum einen nicht von vornherein wissen, welche Internetzugänge der überwachte Teilnehmende benutzen wird und zum anderen sehr viele Internetzugänge (z. B. WLAN-Zugangspunkte) in Frage kommen können, ist es effizienter, die Überwachung bei der Anbieterin der Anwendung (im Beispiel bei der Anbieterin des Internettelefoniedienstes) vorzunehmen. Dadurch werden alle Kommunikationen erfasst, die über den überwachten Internettelefoniedienst geführt werden, unabhängig davon, welchen Netzzugang die überwachte Person benutzt. Die Anbieterin hat zudem eine allfällige von ihr angebrachte Verschlüsselung zu entfernen. So werden die überwachten Kommunikationsinhalte für die Strafverfolgungsbehörden auch auswertbar.

Da die Produkte der Anbieterinnen mehrere Dienstkategorien umfassen können (z. B. Mobilfunkabonnement mit der Dienstkategorie Netzzugang und der Dienstkategorie Telefonie- und Multimediadienste), kann es für eine vollständige Überwachung erforderlich sein, dass mehrere Überwachungstypen für den gleichen zu überwachenden Identifikator (Target ID) angeordnet werden müssen. Zu beachten ist des Weiteren, dass Fernmeldeprodukte mehrere unterschiedliche Dienstangebote enthalten können, welche zu verschiedenen Überwachungstypen gehören. Wenn beispielsweise ein Smartphone komplett in Echtzeit überwacht werden soll (Inhalt und Randdaten), muss die Behörde zwei Überwachungen anordnen: (die erste vom Typ RT_23_NA_CC_IRI für den mobilen Internetzugang und die zweite vom Typ RT_25_TEL_CC_IRI für den Mobiltelefoniedienst). Diese Trennung hat eine administrative und eine technische Ursache. In administrativer Hinsicht soll es den anordnenden Behörden wie bisher ermöglicht werden, die Überwachungen der einzelnen Fernmeldedienste entsprechend den Bedürfnissen der Untersuchung unabhängig voneinander anordnen zu können. Technisch gesehen unterscheidet sich die Überwachung des mobilen Internetzugangs grundsätzlich von der Überwachung der Anwendung Mobiltelefonie. Durch die Trennung in zwei verschiedene Überwachungstypen wird den unterschiedlichen Abläufen bei der Aktivierung und Durchführung der Überwachungen auf Seiten der Mitwirkungspflichtigen Rechnung getragen.

2. Abschnitt: Qualitätssicherung

Art. 29 Qualität der übermittelten Daten

Damit ein reibungsloser Ablauf der Überwachung nicht beeinträchtigt wird, muss unter anderem auch die Qualität der übermittelten Daten gewahrt sein. Diese Bestimmung definiert deshalb die Anforderungen an die Qualität der übermittelten Daten.

Absatz 1 führt drei kumulative Anforderungen an die Qualität der übermittelten Daten auf. Zu *Buchstabe b* sei angemerkt, dass nur die Ausleitung der Überwachungs- beziehungsweise Auskunftsdaten ohne Datenverlust und ohne Unterbrüche erfolgen muss. Die Qualität der Überwachungsdaten kann daher nicht besser sein, als die der vorschriftsmässig überwachten Dienste. Ebenso kann die Qualität der Auskunftsdaten nicht besser sein, als die der vorschriftsmässig erfassten und gespeicherten Bestands- und Randdaten.

Absatz 2 regelt die Verantwortlichkeiten bei der Sicherstellung der Qualität. Für die Qualität der übermittelten Auskunfts- und Überwachungsdaten ist somit bis zum Übergangspunkt die Mitwirkungspflichtige verantwortlich (Art. 12 Abs. 3 BÜPF). Einzelheiten zum Übergangspunkt finden sich in Anhang 2 zur VD-ÜPF. Der Dienst ÜPF steht der betreffenden Mitwirkungspflichtigen dabei beratend zur Seite. Eine Mitwirkungspflichtige ist auch dann für die Qualität der übermittelten Daten verantwortlich, wenn sie Dritte mit der Ausführung der Überwachung beauftragt hat.

Stellt der Dienst ÜPF oder die betreffende Mitwirkungspflichtige fest, dass die Qualität der übermittelten Daten mangelhaft ist, haben sie sich unverzüglich gegenseitig zu informieren (*Abs. 3*). Falls insbesondere Leistungen betroffen sind, die während des Pikettdienstes erbracht werden (s. Art. 11) hat diese Meldung sofort telefonisch an die entsprechenden Kontaktstellen zu erfolgen. Denkbar ist auch, dass Qualitätsmängel durch die Strafverfolgungsbehörden festgestellt werden. In diesem Fall hat die betreffende Strafverfolgungsbehörde den festgestellten Mangel an den Dienst ÜPF zu melden und dieser informiert anschliessend die betreffende Mitwirkungspflichtige.

Sowohl der Dienst ÜPF als auch die Mitwirkungspflichtigen mit Überwachungspflichten betreiben ein Monitoring zur Qualitätskontrolle. Die Details sind in der VD-ÜPF geregelt. Die Mitwirkungspflichtigen mit Überwachungspflichten sind die FDA, ausser jenen mit reduzierten Überwachungspflichten gemäss Artikel 51, und die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten gemäss Artikel 52.

Bei Störungen analysieren die betreffende Mitwirkungspflichtige und der Dienst ÜPF diese unverzüglich und informieren die Gegenpartei umfassend und schnellstmöglich über die Analyseergebnisse. Liegt die Störung auf Seiten der Mitwirkungspflichtigen, hat sie dem Dienst ÜPF eine formelle Störungsmeldung in schriftlicher Form unter Angabe des genauen Ausfallzeitraums, der Problembeschreibung, einer chronologischen Übersicht der eingeleiteten Massnahmen und des Problemstatus zukommen zu lassen. Die Störungsmeldung hat dabei spätestens am nächsten Arbeitstag zu erfolgen. Die Mitwirkungspflichtige hat zudem dem Dienst ÜPF so rasch wie möglich mitzuteilen, wie lange die Störung nach ihrer Einschätzung dauern wird. Zur

umfassenden Information gehört auch die Übermittlung der einzelnen Abklärungsergebnisse und der dazugehörigen Daten an die Gegenseite. Diese Daten dienen zur Untermauerung der Analyseergebnisse und werden gegebenenfalls von der Gegenseite für ihre Analyse benötigt. Der Dienst ÜPF hört die betreffende Mitwirkungspflichtige an und legt gemeinsam mit dieser den jeweiligen Schweregrad (z. B.: kritisch, schwerwiegend, geringfügig) der Störung fest. Die betreffende Mitwirkungspflichtige behebt die festgestellten Mängel innerhalb der durch das EJPD für die einzelnen Schweregrade festgelegten Reparaturzeiten und informiert den Dienst ÜPF schriftlich und regelmässig in den durch das EJPD festgelegten Zeitabständen über die weiteren eingeleiteten Massnahmen und den neusten Problemstatus. Nach der Störungsbehebung hat die Anbieterin dem Dienst ÜPF unverzüglich eine schriftliche Abschlussmeldung zu senden, welche die Angaben der Störungsmeldung vervollständigt und gegebenenfalls präzisiert.

Die Randdaten der Echtzeitüberwachung sind gemäss den technischen Möglichkeiten der Schnittstellenspezifikation zu speichern und unverzüglich nachzuliefern. Sollten die Randdaten der Echtzeitüberwachung nicht mehr verfügbar oder unvollständig sein, hat die Mitwirkungspflichtige auf Anweisung des Dienstes ÜPF die entsprechenden Randdaten der rückwirkenden Überwachung unverzüglich zu liefern (s. Art. 4 Abs. 3).

Art. 30 Testschaltungen

Unter einer *Testschaltung* versteht man die technische Überwachung eines Fernmeldedienstes (z. B. Mobiltefonie, Mobiler Internetzugang, E-Mail-Konto) beziehungsweise abgeleiteten Kommunikationsdienstes (z. B. Instant Messaging, Chatdienst) zu den in Absatz 1 aufgeführten Zwecken. Die dabei verwendeten Geräte und Software werden als *Testausstattung* bezeichnet. Dies können beispielsweise Endgeräte wie Smartphones sein oder auch Simulatoren in Form von Software, welche die testende Organisation ausschliesslich zu diesem Zweck einsetzt. Bei einer Testschaltung wird das Ziel der Überwachung als *Testtarget* bezeichnet. Die im Rahmen einer Testschaltung verwendeten beziehungsweise erzeugten Daten (z. B. Telefongespräche, SMS, Internetverkehr) werden als *Testdaten* bezeichnet. Die *Testdaten* werden unter Kenntnisnahme aller Beteiligten lediglich mit dem Ziel verwendet oder erzeugt, um die unter Absatz 1 aufgeführten Zwecke zu erfüllen. Damit wird sichergestellt, dass alle an einer Testüberwachung beteiligten Kommunikationspartner und deren Fernmeldeverkehr nur fiktiv sind. Testtargets, Testdienste und Testausstattungen stehen nur denjenigen Personen des Dienstes ÜPF, der Mitwirkungspflichtigen, der Strafverfolgungsbehörden und des NDB zur Verfügung, die zur Benutzung von Testschaltungen berechtigt sind.

Da die Testdaten lediglich für Testschaltungen benutzt werden, fallen sie nicht unter das Fernmeldegeheimnis. Testschaltungen bedürfen somit auch keiner Genehmigung durch die Genehmigungsbehörde und auch die Voraussetzungen von Artikel 269 Absatz 1 StPO beziehungsweise Artikel 70 Absatz 21MStP müssen nicht erfüllt sein. Da es bei Testschaltungen des Dienstes ÜPF keine mit dem Verfahren befasste Behörde gib, kann der Dienst ÜPF vom Inhalt der Testdaten seiner eigenen Testschaltungen Kenntnis nehmen, ohne eine vorgängige Zustimmung einholen zu müssen (Art. 18 Abs. 2 BÜPF).

Für Testschaltungen führt der Dienst ÜPF gesonderte Überwachungsakten im Sinne von Artikel 9. Bei Testschaltungen erfasst der Dienst ÜPF lediglich die Angaben zur verantwortlichen Person, deren Organisationseinheit (Name und Adresse), den Verwendungszweck der Testschaltung und die Namen der berechtigten Personen, welche die Daten der Testschaltung bearbeiten dürfen. Hingegen werden auch Testschaltungen ähnlich wie normale Überwachungen protokolliert. Der Dienst ÜPF protokolliert also auch bei Testschaltungen die Datenbearbeitung aller Testschaltungen. Der Dienst ÜPF verwaltet auch eine Anzahl von Testschaltungen, die er den Strafverfolgungsbehörden und dem NDB im Rahmen von Testarbeiten oder Schulungen zur Verfügung stellen kann. Diese gelten als kostenlose Testschaltungen des Dienstes ÜPF. Die den Behörden zur Verfügung gestellten kostenlosen Testschaltungen des Dienstes ÜPF verursachen auch keinerlei Kosten für die dafür erforderlichen Fernmeldedienste beziehungsweise abgeleiteten Kommunikationsdienste, sofern die Regeln zur angemessenen Verwendung eingehalten werden. Aussergewöhnlich kostenintensive Nutzungen müssen vorgängig gesondert mit dem Dienst ÜPF vereinbart werden. Bei Nichtbeachtung behält sich der Dienst ÜPF Regressforderungen vor.

Beim Überwachungsauftrag an die Mitwirkungspflichtige hat der Dienst ÜPF den Vermerk anzubringen, dass es sich im konkreten Fall um eine Testschaltung handelt. Ist der Dienst ÜPF bei der Erzeugung von Testdaten auf die Hilfe der Mitwirkungspflichtigen angewiesen, kann er sie entsprechend damit beauftragen und erstellt nach Anhörung dieser ein Testkonzept (*Abs. 2*). Des Weiteren muss die Mitwirkungspflichtige dem Dienst ÜPF die für dessen Testschaltungen erforderlichen eigenen Fernmeldedienste beziehungsweise abgeleiteten Kommunikationsdienste kostenlos und dauerhaft zur Verfügung stellen (*Abs. 3*). Das bedeutet, dass namentlich die Grundgebühren, die Aktivierungsgebühren, die wiederkehrenden Gebühren sowie alle Arten von Kommunikations- und Nutzungsgebühren dieser Dienste durch die Mitwirkungspflichtige zu finanzieren sind. So zum Beispiel: Die Mitwirkungspflichtige stellt dem Dienst ÜPF die erforderliche Anzahl von SIM-Karten kostenlos zur Verfügung, aktiviert kostenlos die erforderlichen Dienste und berechnet für deren Nutzung keinerlei Gebühren.

Die Nutzung der Testschaltungen unterliegt den Regeln zur angemessenen Verwendung. Aussergewöhnlich kostenintensive Nutzungen müssen vorgängig gesondert zwischen dem Dienst ÜPF und den betroffenen Mitwirkungspflichtigen vereinbart werden.

Die nicht-proprietären, das heisst marktüblichen Endgeräte werden dagegen vom Dienst ÜPF beschafft und finanziert. Falls die Fernmeldedienste beziehungsweise die abgeleiteten Kommunikationsdienste einer Mitwirkungspflichtigen jedoch proprietäre Endgeräte erfordern, hat sie diese für die Testschaltungen des Dienstes ÜPF erforderlichen Endgeräte ebenfalls kostenlos dem Dienst ÜPF zur Verfügung zu stellen.

Die Strafverfolgungsbehörden und der NDB können gemäss *Absatz 4*, zusätzlich zu Testschaltungen, die ihnen der Dienst ÜPF kostenlos zur Verfügung stellen kann, ebenfalls Testschaltungen auf eigene Kosten durchführen, um die Qualität des ausgeleiteten Fernmeldeverkehrs sicherzustellen und für Schulungszwecke. Es gibt also einerseits die kostenlosen Testschaltungen des Dienstes ÜPF (Abs. 3) und andererseits die kostenpflichtigen Testschaltungen der Strafverfolgungsbehörden und des NDB (Abs. 4). Voraussetzung für die Beantragung eigener

Testschaltungen ist, dass die Strafverfolgungsbehörde respektive der NDB eine Person und deren Stellvertretung benennt, welche für die Verwaltung von Testtargets, Testdiensten und Testausstattungen der betreffenden Organisationseinheit verantwortlich sind und berechtigt sind, beim Dienst ÜPF die erforderlichen Anträge für Testschaltungen einzureichen. Auf eigene Kosten bedeutet, dass die betreffenden Strafverfolgungsbehörden und der NDB für die Durchführung ihrer Testschaltungen dem Dienst ÜPF die entsprechenden Gebühren gemäss Gebührenverordnung zahlen, inklusive der an die beteiligten Mitwirkungspflichtigen zu entrichtenden Entschädigungen. Die anfallenden Gebühren und Entschädigungen sind in der GebV-ÜPF geregelt. Die Strafverfolgungsbehörden und der NDB tragen auch selbst die Kosten der für ihre Testschaltungen erforderlichen Fernmeldedienste beziehungsweise abgeleiteten Kommunikationsdienste und der Endgeräte. Die aus ihren Testschaltungen gewonnenen Testdaten können sie entweder auf das Verarbeitungssystem des Dienstes ÜPF ausleiten lassen oder eine direkte Ausleitung an sich selber veranlassen. Für den Zugriff des Dienstes ÜPF auf Daten aus Testschaltungen der Strafverfolgungsbehörden respektive des NDB gilt Artikel 18 Absatz 2 BÜPF sinngemäss.

Testschaltungen, die auf Ersuchen der Strafverfolgungsbehörden respektive des NDB durchgeführt werden (Testschaltungen der Behörden), müssen ähnlich den gewöhnlichen Überwachungen einen formellen Weg durchlaufen. Die betreffende Behörde muss zuerst beim Dienst ÜPF einen entsprechenden Antrag einreichen. Darin sind Verwendungszweck, Überwachungstyp und Dauer der Testschaltung anzugeben, wobei die Maximaldauer 12 Monate beträgt. Der Dienst ÜPF prüft, ob der Antrag seinen Vorgaben entspricht und, ob dieser von einer dazu berechtigten Person eingereicht wurde. Sind die erwähnten Voraussetzungen erfüllt, übermittelt der Dienst ÜPF die entsprechenden Überwachungsaufträge mit dem Vermerk, dass es sich um Testschaltungen der Behörden handelt, zur Aktivierung der Testschaltungen an die betreffenden Mitwirkungspflichtigen. Die berechtigten Personen der Behörden können auf Antrag ihre Testschaltungen jeweils für maximal weitere 12 Monate gebührenpflichtig verlängern lassen. Der Dienst ÜPF sendet spätestens 3 Monate vor Ablauf einer Testschaltung eine entsprechende Erinnerungsmeldung an die berechtigten Personen der Behörde, die die betreffende Testschaltung beantragt hat. Sind die erwähnten Voraussetzungen für die Verlängerung erfüllt, bleibt die betreffende Testschaltung aktiv. Andernfalls beendet der Dienst ÜPF die betreffende Testschaltung, indem er den Überwachungsauftrag zur termingerechten Aufhebung der Testschaltung an die betreffende Mitwirkungspflichtige übermittelt.

3. Abschnitt: Sicherstellung der Auskunfts- und Überwachungsbereitschaft

Art. 31 Überprüfung der Auskunfts- und Überwachungsbereitschaft

Auskunftsbereitschaft bedeutet, dass die folgenden Mitwirkungspflichtigen in der Lage sind, die folgenden Auskünfte, die durch sie angebotene Dienste betreffen, zu erteilen oder sie durch Dritte erteilen zu lassen (vgl. Art. 18):

- Die FDA und die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten gemäss Artikel 22: die Auskünfte gemäss den Artikeln 35-37 und 40-48 sowie gemäss Artikel 27 in Verbindung mit den Artikeln 35, 40, 42 und 43
- Die FDA, ausser jenen mit reduzierten Überwachungspflichten gemäss Artikel 51, und die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten gemäss Artikel 52: die Auskünfte gemäss den Artikeln 38 und 39.

Überwachungsbereitschaft bedeutet, dass die folgenden Mitwirkungspflichtigen in der Lage sind, die folgenden Überwachungen, die durch sie angebotene Dienste betreffen, auszuführen oder sie durch Dritte ausführen zu lassen (vgl. Art. 50):

- Die FDA, ausser jenen mit reduzierten Überwachungspflichten gemäss Artikel 51, und die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten gemäss Artikel 52: die Überwachungen gemäss Artikel 54-68.

Um die Auskunfts- beziehungsweise Überwachungsbereitschaft zu belegen, müssen die erwähnten Anbieterinnen neu nachweisen, dass sie die Erteilung der Auskünfte beziehungsweise die Ausführung der Überwachungen nach dem anwendbaren Recht sicherstellen können (*Abs. 1*).

Gemäss *Absatz 2* ist der Nachweis erbracht, wenn die gemäss den Vorgaben des Dienstes ÜPF durchzuführenden Tests erfolgreich abgeschlossen worden sind (*Bst. a*) und die Anbieterin in einem vom Dienst ÜPF erarbeiteten Fragebogen bestätigt, dass sie die Vorgaben bezüglich der standardisierten Auskünfte beziehungsweise Überwachungen erfüllt, die nicht mittels Tests nachgewiesen werden. Da die Anbieterinnen die Möglichkeit haben, die ihnen zukommenden Auskunfts- und Überwachungspflichten durch Dritte erfüllen zu lassen, können sie auch Dritte mit dem Nachweis der Auskunfts- und Überwachungsbereitschaft beauftragen. Die Verantwortung für den Nachweis liegt in jedem Fall bei der betreffenden Anbieterin.

Bei der Überprüfung der Auskunfts- und Überwachungsbereitschaft nimmt der Dienst ÜPF die Aufgaben gemäss *Absatz 3* wahr. Die Protokolle (*Bst. e*) können einerseits im Falle eines Rechtsstreits als Beweismittel herangezogen werden, andererseits können sie bei der nächsten Überprüfung der Auskunfts- und Überwachungsbereitschaft als Hilfsmittel dienen.

Da jede Anbieterin andere Dienste anbietet, legt der Dienst ÜPF nach *Absatz 4* die Bestätigung für jede Anbieterin individuell mit bestimmten Gültigkeitskriterien für die Datenausleitung gemäss den Vorgaben des Departements fest. Zu diesen Gültigkeitskriterien gehören unter anderem die Angaben zu den getesteten Systemen, zu den getesteten Diensten und Überwachungstypen, die Testprotokolle mit Anhängen und die Schnittstellen. Es werden sowohl die Systeme des Dienstes ÜPF (ADMF[42], LEMF[43]) wie auch diejenigen der Anbieterinnen (ADMF, MF[44]/DF[45], IIF[46]) getestet. Beim Testen der Dienste, wie der Telefonie, wird auch

42 ADMinistration Function (vgl. ETSI TS 101 671)
43 Law Enforcement Monitoring Facility (vgl. ETSI TS 101 671)
44 Mediation Function (vgl. ETSI TS 101 671)
45 Distribution Function (vgl. ETSI TS 101 671)
46 Internal Interception Function (vgl. ETSI TS 101 671)

die Art der Technologie, wie VoLTE, getestet. Teste bei den Überwachungstypen finden grundsätzlich für Echtzeitüberwachungen (wie RT_24_TEL_IRI, RT_25_TEL_CC_IRI) statt.

Art. 32 Gültigkeitsdauer der Bestätigung

Hier ist einleitend anzumerken, dass die nach bisheriger Praxis vom Dienst ÜPF erteilten Bestätigungen, sogenannte "Statement of Compliance" oder "Confirmation of Compliance", nicht als Bestätigung der Auskunfts- und Überwachungsbereitschaft im Sinne von Artikel 33 Absatz 6 BÜPF gelten.

Sobald der Nachweis der Auskunfts- beziehungsweise Überwachungsbereitschaft erbracht wurde (s. Erläuterungen zu Art. 31), stellt der Dienst ÜPF der betreffenden Mitwirkungspflichtigen eine Bestätigung aus, die gemäss *Absatz 1* während 3 Jahren gültig ist. Massgebend für die Fristberechnung ist dabei das Ausstelldatum der Bestätigung durch den Dienst ÜPF.

Absatz 2 sieht vor, dass der Dienst ÜPF nach Ablauf der Gültigkeitsdauer die Bestätigung jeweils um weitere drei Jahre verlängern kann, wenn die Mitwirkungspflichtige bescheinigt, dass seit der Erteilung der Bestätigung keine Umstellungen vorgenommen wurden, welche die Datenausleitung, die Auskunfts- oder die Überwachungsbereitschaft beeinflussen. Hierfür muss die Mitwirkungspflichtige beim Dienst ÜPF einen entsprechenden Antrag stellen und die unter Absatz 2 aufgeführten Bescheinigungen beilegen.

Absatz 3 auferlegt der Mitwirkungspflichtigen eine Meldepflicht. Die Mitwirkungspflichtige hat demnach die Pflicht, den Dienst ÜPF unverzüglich darüber in Kenntnis zu setzen, falls sie feststellt, dass sie nicht mehr auskunfts- oder überwachungsbereit ist.

Art. 33 Abnahmeverfahren

Diese Bestimmung gibt dem EJPD die Kompetenz, den Ablauf des Verfahrens für die Abnahme der technischen Systeme sowie das Verfahren zur Überprüfung der Auskunfts- und Überwachungsbereitschaft zu regeln (s. auch Art. 31 Abs. 3 BÜPF).

Art. 34 Ungültigerklärung der Bestätigung der Auskunfts- und Überwachungsbereitschaft

Ist eine FDA, eine Anbieterin abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten oder eine Anbieterin abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten nicht mehr in der Lage, die Auskünfte beziehungsweise die Überwachungen, die durch sie angebotene Dienste betreffen, zu erteilen beziehungsweise auszuführen, erklärt der Dienst ÜPF die bereits durch ihn erteilte Bestätigung der Auskunfts- beziehungsweise Überwachungsbereitschaft unverzüglich für ungültig. Es ist möglich, dass die Anbieterin nur in Bezug auf bestimmte von ihr angebotene Dienste nicht mehr auskunfts- und/oder überwachungsbereit ist. In diesem Fall bezieht sich die Ungültigerklärung lediglich auf den betreffenden Dienst und den nicht mehr sichergestellten Auskunfts- und/oder Überwachungstyp. Die Ungültigerklärung bezieht sich nicht auf die anderen von der Anbieterin angebotenen Dienste. In einem solchen Fall ist, in Bezug auf jene Dienste, bei

denen die Auskunfts- und Überwachungsbereitschaft gewährleistet ist, eine separate Bestätigung zu erstellen. Bei Bedarf kann auch in diesem Fall eine erneute Überprüfung angeordnet werden, bevor eine allfällige Bestätigung ausgestellt wird. Aus dieser Bestätigung muss klar hervorgehen, auf welche Dienste sich die Bestätigung bezieht. Ist in Bezug auf einen angebotenen Dienst die Auskunftsbereitschaft zwar gegeben, jedoch nicht die Überwachungsbereitschaft, ist dies ebenfalls in der Bestätigung beziehungsweise in der Ungültigerklärung entsprechend festzuhalten.

Eine Ungültigerklärung wird dann in Erwägung gezogen, wenn die Anbieterin selbst einen entsprechenden Antrag stellt (*Bst. a*), wenn die Anbieterin in mehreren Fällen nicht in der Lage ist, die Datenausleitung, die Auskunfts- oder die Überwachungsbereitschaft sicherzustellen (*Bst. b*) oder wenn bestätigte Aussagen der Anbieterin nicht der Wahrheit entsprechen (*Bst. c*).

4. Abschnitt: Auskunftstypen für Netzzugangsdienste

Art. 35 Auskunftstyp IR_4_NA: Auskünfte über Teilnehmende von Netzzugangsdiensten

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Teilnehmende von Netzzugangsdiensten. Dieser Auskunftstyp entspricht im Wesentlichen den bisherigen Auskünften A0 und teilweise A1 (*Abs. 2 Bst. j und k*). Möglich sind neu Abfragen nach der Unternehmens-Identifikationsnummer (*Abs. 2 Bst. g*), dem Teilnehmeridentifikator (*Abs. 2 Bst. h*) und dem Dienstidentifikator (*Abs. 2* Bst. i).

Unter Netzzugangsdiensten sind Fernmeldedienste zu verstehen, die unmittelbar (z. B. DSL-Internetanschluss) oder mittelbar (z. B. Virtual Private Network, VPN) den Zugang zu öffentlichen Fernmeldenetzen wie dem Internet ermöglichen. Beim VPN ist Folgendes zu beachten: Zwischen dem unmittelbaren Internetzugang des VPN-Kunden und der VPN-Anbieterin besteht ein VPN-Tunnel. Die VPN-Kunden treten im Internet mit einer IP-Adresse der VPN-Anbieterin auf und nicht mit der von ihrer unmittelbaren Internet-Zugangsanbieterin zugeteilten IP-Adresse, das heisst die Zugriffe der VPN-Kunden ins Internet haben als Quelladresse eine IP-Adresse der VPN-Anbieterin. Die IP-Adresse des unmittelbaren Internetzugangs der VPN-Kunden ist nur für die VPN-Anbieterin sichtbar. Daher müssen die VPN-Anbieterinnen ebenfalls Auskünfte über ihre Teilnehmenden und Dienste geben können.

Dieser Auskunftstyp ist nach dem ETSI-Standard TS 102 657 aufgebaut. Er kombiniert die allgemeinen Teilnehmendeninformationen (generic subscriber info) mit den wichtigsten Angaben zu den Netzzugangsdiensten des Teilnehmenden. Weitere spezifische Angaben über Netzzugangsdienste können über den Auskunftstyp IR_6_NA (Art. 36) abgefragt werden.

Der Artikel kann mit einem Beispiel veranschaulicht werden: Die Person X bezieht die folgenden Dienste bei der Anbieterin Y: drei Mobilabonnemente (mit Telefonie und Internet), zehn Prepaid-Karten (nur Telefonie) und zwei Internetzugangsdienste im Festnetz. Die Strafverfolgungsbehörde, die den Namen und die Adresse

der Person X kennt, möchte wissen, welche Dienste die Person X bei der Anbieterin Y bezieht. Zu diesem Zweck stellt sie die Auskunftsgesuche IR_4_NA (Art. 35) und IR_10_TEL (Art. 40). Anbieterin Y antwortet zum Auskunftstyp IR_4_NA (Art. 35) mit fünf Ergebnissen (zählt als fünf Datensätze, s. die Erläuterungen zu Art. 17 Abs. 4) und zum Auskunftstyp IR_10_TEL (Art. 40) mit 13 Ergebnissen (zählt ebenfalls als 13 Datensätze).

In *Absatz 1* werden die in der Antwort zu liefernden Angaben über Teilnehmende von Netzzugangsdiensten aufgeführt; siehe Artikel 21 Absatz 1 BÜPF (Auskünfte über Fernmeldedienste) und Artikel 22 Absatz 2 und 4 BÜPF (Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet).

Gemäss *Buchstabe a* ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin dem Teilnehmenden einen solchen zugeteilt hat.

Die in *Buchstabe b* aufgeführten Angaben zur Person werden im Einzelnen bei Artikel 20 erläutert.

Nachfolgend werden die einzelnen Ziffern des *Buchstabens c* erläutert:

- Bei dem in *Ziffer 1* genannten "eindeutigen Identifikator, welcher die Anbieterin bezeichnet", handelt es sich um eine administrative Nummer, die der Dienst ÜPF der Anbieterin zuteilt, um sie eindeutig zu identifizieren.

- Der "eindeutige Dienstidentifikator" gemäss *Ziffer 2* bezeichnet den in Anspruch genommenen Fernmelde- oder abgeleiteten Kommunikationsdienst des Teilnehmenden. Diese Bezeichnung muss mindestens im Bereich der Anbieterin eindeutig sein (z. B. Telefonnummer, Benutzername, Bezeichnung des Breitbandanschlusses, E-Mail-Adresse).

- Unter dem Begriff *Beginn* des "Zeitraums des Dienstbezugs" gemäss *Ziffer 3* ist der Zeitpunkt (Datum und Uhrzeit) der Aufnahme der Kundenbeziehung zu verstehen. Die eigentliche Aktivierung des Dienstes kann unter Umständen später erfolgt sein. So ist es möglich, dass z. B. eine Prepaid-SIM-Karte an einem Tag verkauft und die dazugehörigen Personendaten am selben Tag erfasst wurden, die SIM-Karte jedoch erst einige Tage später aktiviert wurde. Aktivierung bedeutet in diesem Sinne, dass der Dienst ab diesem Zeitpunkt für den Teilnehmenden nutzbar ist. Falls zutreffend ist der Zeitpunkt der Aktivierung mitzuteilen.

  Hinweis: In dieser Verordnung bedeutet die Formulierung "falls zutreffend" (if applicable), dass die entsprechende Regelung nur auf den entsprechenden Anwendungsfall zutrifft, z. B. eine SIM-Nummer (ICCID) kann nur geliefert werden, wenn es sich um einen Mobilfunkdienst handelt. Es kann dann trotzdem vorkommen, dass die SIM-Nummer bei einem Mobilfunkdienst in einem speziellen Szenario nicht vorhanden ist.

  Das *Ende-Datum* bezeichnet den Zeitpunkt, ab dem der Dienst für den Teilnehmenden dauerhaft nicht mehr nutzbar ist. Eine vorübergehende Sperrung des Dienstes gilt hingegen nicht als Ende des Dienstbezugs. Der Zusatz "gegebenenfalls" bedeutet, dass nur dann ein *Ende-Datum* zu liefern ist, wenn der Dienst für den Teilnehmenden dauerhaft nicht mehr nutzbar ist.

- Gemäss *Ziffer 4* können optional Angaben über zusätzliche Optionen oder Einschränkungen des Netzzugangsdienstes in für Menschen lesbarer Form

übermittelt werden, z. B. "mit statischer IP-Adresse", "Datenvolumen max. 1 GB" (s. ETSI-Standard TS 102 657, Tabelle E.2).

- Die Standortangaben des Festnetzzugangs gemäss *Ziffer 5* bestehen aus der Installationsadresse des Netzzugangs, wie sie die Anbieterin für den Teilnehmenden vermerkt hat.

- Bei den Zuständen des Dienstes gemäss *Ziffer 6* kann die Anbieterin die bei ihr üblichen Bezeichnungen übermitteln, da eine Umwandlung in standardisierte Bezeichnungen zu viel Aufwand verursachen würde. Mit Gültigkeitszeitraum ist die Zeitspanne (Beginn-Datum und gegebenenfalls End-Datum) gemeint, von wann bis wann die Zustandsangabe gültig ist beziehungsweise war.

- Gemäss *Ziffer 7*, falls zutreffend, alle im Zusammenhang mit diesem Dienst zugeteilten statischen IP-Adressen, IP-Präfixe, IP-Adressbereiche und Netzmasken beziehungsweise Präfixlängen und jeweils deren Gültigkeitszeitraum.

- Gemäss *Ziffer 8* sind im Falle von kostenlosen oder vorbezahlten Fernmeldediensten (Prepaid) zusätzlich gemäss Artikel 21 Absatz 1 Buchstabe e BÜPF und Artikel 20 Absatz 1 die Abgabestelle und der Name der Person, die das für den Zugang zum Fernmeldedienst erforderliche Mittel abgegeben hat, mitzuteilen.

- Gemäss *Ziffer 9* sind, falls zutreffend, alle im Zusammenhang mit dem angefragten Netzzugangsdienst durch die Anbieterin in den Bestandsdaten registrierten Nummern der SIM-Karten (ICCID) und deren Aktivierungs- und gegebenenfalls Deaktivierungsdatum zu liefern.

- Gemäss *Ziffer 10* ist im Falle von Mobilfunkdiensten die IMSI (International Mobile Subscriber Identity) zu liefern. Diese global eindeutige Nummer dient zur Identifikation des Mobilfunk-Teilnehmenden gegenüber dem Netz.

- Gemäss *Ziffer 11* ist der Typ des Dienstes zu liefern. Diese Angabe dient zur Mitteilung, ob es sich um einen vorbezahlten Dienst (prepaid) oder ein Abonnement handelt (postpaid).

- Gemäss *Ziffer 12* ist, falls zutreffend, der alternative Teilnehmeridentifikator für den Netzzugangsdienst zu liefern. Diese Angabe ist nur dann erforderlich, falls es neben dem eindeutigen Teilnehmeridentifikator gemäss Buchstabe a noch einen weiteren Teilnehmeridentifikator für diesen Netzzugangsdienst gibt.

In *Absatz 2* sind die Anfragekriterien aufgeführt. Mit diesen erfolgt die Anfrage durch die Strafverfolgungsbehörde an die Anbieterin über das Auskunftssystem des Dienstes ÜPF. Dabei muss mindestens ein Anfragekriterium im Auskunftsgesuch angegeben werden. Bei Verwendung eines Anfragekriteriums gemäss den Buchstaben a bis d ist noch ein weiteres Anfragekriterium (*Bst. a-k*) anzugeben, damit die Anfrage spezifisch genug ist. Die Anfragekriterien gemäss den *Buchstaben e-k* sind hingegen eindeutig, so dass die Angabe **eines** solchen Anfragekriteriums bereits ausreicht. Bei einer Suche nach Zeichenketten (*Bst. a, c, d und e*) hat die Anbieterin eine sogenannte buchstabengetreue Suche gemäss Artikel 13 Absatz 1 VD-ÜPF durchzuführen. Damit ist im Prinzip eine exakte Suche gemeint, jedoch werden die gesuchte Zeichenkette und die Zeichenketten,

mit denen bei der Suche verglichen wird, wie folgt normalisiert: Buchstaben, die nicht Teil des aus 26 Buchstaben bestehenden lateinischen Alphabets sind, werden vor Ausführung der Suche gestützt auf eine Umsetzungsliste in 1 beziehungsweise 2 Buchstaben aus dem lateinischen Alphabet umgewandelt. Eine hundertprozentig exakte Suche würde in der Praxis häufig nicht zu den gewünschten Ergebnissen führen, da unterschiedliche Zeichensätze verwendet werden, die nicht alle Zeichen darstellen können, und Interpunktionszeichen in Namen häufig falsch verwendet oder vergessen werden.

In *Buchstabe a* sind Name(n) und Vorname(n) zu einem Anfragekriterium zusammengefasst. Dies ermöglicht eine freie Kombination bei der Anfrage. Einerseits kann es vorkommen, dass bei der Registrierung Vornamen und Nachnamen bei der Erfassung vertauscht werden; anderseits ist es nicht immer klar, welches der Vorname beziehungsweise der Nachname ist (z. B. Thomas Peter), oder eine Person hat mehrere Vornamen beziehungsweise Nachnamen (z. B. Heydi Núñez Gómez).

Hausnummern sind nicht immer vorhanden, daher der Zusatz *allenfalls* in *Buchstabe d*.

In *Buchstabe i* sind IP-Adressen als Anfragekriterium ausgeschlossen, da für die Abfrage von IP-Adressen die spezifischen Auskunftstypen IR_7_IP (Art. 37), IR_8_IP_NAT (Art. 38) und IR_9_NAT (Art. 39) zur Verfügung stehen (s. die Erläuterungen zu Art. 37, 38 und 39).

Art. 36 Auskunftstyp IR_6_NA: Auskünfte über Netzzugangsdienste

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Netzzugangsdienste, der auf dem ETSI-Standard TS 102 657 basiert. Damit werden weitere Angaben gemäss Artikel 21 Absatz 1 Buchstabe d BÜPF eingeholt.

In *Absatz 1* sind die in der Antwort zu liefernden Angaben und in *Absatz 2* die Anfragekriterien aufgeführt.

Bei Absatz 1 *Buchstabe d* ist zu beachten, dass die Liste der im Anfragezeitraum **tatsächlich benutzten** Geräteidentifikatoren zu liefern ist. Diese Informationen hat die Anbieterin aus den gespeicherten Randdaten zu gewinnen, ohne jedoch die Randdaten selbst herauszugeben (zum Begriff Randdaten, s. auch die einleitenden Erläuterungen zum 10. Abschnitt des 3. Kapitels), sofern die Anbieterin Überwachungspflichten hat. Anbieterinnen ohne Überwachungspflichten liefern die vorhandenen Daten. Aus der Antwort darf nicht ersichtlich sein, wann, wie und wo die Benutzung des Geräts im Einzelnen stattgefunden hat.

Der in der Antwort angegebene Gültigkeitszeitraum bezieht sich auf die drei Parameter gemäss den Buchstaben b (Dienstidentifikator), c (IMSI und MSISDN) und e (SIM-Nummer) von Absatz 1 gemeinsam. Wie bereits ausgeführt, bezieht sich dieser Gültigkeitszeitraum nicht auf die Geräteidentifikatoren. Wenn sich einer der drei vorgenannten Parameter innerhalb des in der Anfrage angegebenen Zeitraums geändert hat, hat die Mitwirkungspflichtige dem jeweiligen Stand der Informationen entsprechend mehrere Datensätze zu liefern. Da die PUK-Codes fest mit einer SIM-Karte verknüpft sind, muss für den Antwortparameter gemäss Absatz 1 Buchstabe f (PUK-Code) kein Gültigkeitszeitraum angegeben werden. Dessen Gültigkeit ergibt sich direkt aus der Gültigkeit der SIM-Nummer (*Abs. 1 Bst. e*).

Art. 37 Auskunftstyp IR_7_IP: Identifikation der Benutzerschaft bei eindeutig zugeteilten IP-Adressen

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte zur Identifikation der Benutzerschaft bei eindeutig zugeteilten IP-Adressen, der sich am ETSI-Standard TS 102 657 orientiert. Damit werden die Angaben gemäss Artikel 22 Absatz 2 BÜPF eingeholt. Dieser Auskunftstyp entspricht den bisherigen Auskünften A0.1 (statische IP-Adresse) und A0.2 (dynamische IP-Adresse). In diesem Auskunftstyp werden alle Anfragen nach statischen und eindeutig zugeteilten dynamischen IP-Adressen vereinheitlicht, da man es einer IP-Adresse nicht ansieht, ob sie statisch oder dynamisch zugeteilt war. Ausserdem gibt es noch die nicht-eindeutige Zuteilung von IP-Adressen (s. Art. 38 und 39).

Unter dem Begriff *eindeutig zugeteilte IP-Adresse* ist zu verstehen, dass zu einem beliebigen Zeitpunkt maximal ein Teilnehmender mit dieser Adresse im Internet aufgetreten ist. Dies trifft zum einen auf die statischen IP-Adressen und zum anderen auf die eindeutig zugeteilten dynamischen IP-Adressen zu. Da man es einer IP-Adresse auch nicht ansieht, ob sie eindeutig zugeteilt war, verschafft erst das Ergebnis dieses Auskunftstyps Klarheit.

Wichtig ist einerseits die Angabe eines hinreichend genauen Zeitpunkts im Auskunftsgesuch, da bei IP-Adressen der Zuteilungszeitraum sehr kurz sein kann und damit falschpositive Ergebnisse erzielt werden könnten. Insbesondere bei ausländischen Zeitangaben ist auf die korrekte Zeitzone zu achten. Andererseits sollte ein Toleranzintervall wegen der möglichen Ungenauigkeiten der Systemuhren berücksichtigt werden. Im Auskunftsgesuch kann daher statt eines fixen Zeitpunkts (*Abs. 2 Bst. b*) ein Zeitintervall eingegeben werden.

Wenn ein Auskunftsgesuch des Typs IR_7_IP mehrere Ergebnisse liefert, gibt es dafür zwei mögliche Ursachen, was von der berechtigten Behörde bei der Anbieterin weiter abgeklärt werden muss:

1) Das Zeitintervall im Gesuch ist zu gross. Die fragliche IP-Adresse wurde im Zeitintervall mehreren Teilnehmenden zugeteilt.
2) Die fragliche IP-Adresse war nicht eindeutig zugeteilt.

Im 1. Fall ist das Auskunftsgesuch des Typs IR_7_IP erneut zu stellen, jedoch mit einem kleineren Zeitintervall.

Im 2. Fall ist ein neues Auskunftsgesuch des Typs IR_8_IP (NAT) zu stellen, das jedoch die Angabe weiterer Anfragekriterien erfordert (s. Erläuterungen zu Art. 38).

Wenn ein Auskunftsgesuch des Typs IR_7_IP kein Ergebnis liefert, wurde möglicherweise ein zu kleines Zeitintervall im Gesuch gewählt oder die Zeitangabe war ungenau, zum Beispiel aufgrund einer falschen Zeitzonenumrechnung.

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

Dieser Auskunftstyp ist neu und behandelt ein spezifisches Problem der Teilnehmeridentifikation im Falle von nicht-eindeutig zugeteilten IP-Adressen. Er basiert auf dem ETSI-Standard TS 102 657. Bei der sogenannten Network Address

Translation (NAT) können sich bis zu vielen Tausend Benutzern und Benutzerinnen gemeinsam die gleiche öffentliche IP-Adresse teilen. Eine Teilnehmeridentifikation ist bei NAT daher nur mit erhöhtem technischem Aufwand möglich.

Carrier-grade NAT (cgNAT) bedeutet Network Address Translation (NAT) auf Ebene der Anbieterin (Carrier). Dabei werden den Teilnehmenden im Netz der Zugangsanbieterin private IP-Adressen zugeteilt, die nur innerhalb des Netzes der Zugangsanbieterin gültig sind. Diese werden bei Zugriffen ins Internet an den Netzgrenzen der Zugangsanbieterin zum Internet in eine gemeinsame öffentliche Quell-IP-Adresse übersetzt (viele Teilnehmende teilen sich gleichzeitig eine öffentliche IP-Adresse). Die Unterscheidung der vielen einzelnen Internetverbindungen erfolgt mittels Port-Nummern. Diese Adressübersetzung muss für jedes eingehende und ausgehende IP-Paket durchgeführt werden. Bei nichtdeterministischen Verfahren führt das Gerät (Router) Zuordnungstabellen und speichert für jede Internetverbindung (Kontext) den Zeitstempel, die Quelle und das Ziel der Verbindung (jeweils IP-Adresse und Portnummer), die zugehörige private IP-Adresse und Portnummer des Teilnehmenden sowie die Art des Transportprotokolls. Bei deterministischen NAT-Verfahren werden Adressen und Portnummern mit einem Algorithmus übersetzt und können später wieder zurückgerechnet werden und somit entfällt die Notwendigkeit der Speicherung der IP-Adressen und Portnummern der einzelnen Verbindungsziele durch die Zugangsanbieterin für die Zwecke der Teilnehmeridentifikation. Aus datenschutzrechtlicher Sicht sind Verfahren zu implementieren, bei denen die Speicherung der Verbindungsziele nicht erforderlich und daher zu unterlassen ist.

Für den mobilen Internetzugang (z. B. GPRS, UMTS, LTE) werden schon seit längerem NAT-Verfahren eingesetzt. Die Hauptgründe dafür sind die Knappheit von öffentlichen IPv4-Adressen und Sicherheitsüberlegungen wie das sogenannte Topology Hiding, das heisst damit man von aussen nicht auf die Struktur des Netzes schliessen kann. Da mittlerweile kaum noch öffentliche IPv4-Adressen verfügbar sind, sind die Zugangsanbieterinnen dazu übergegangen, cgNAT mehr und mehr auch für fixe Internetzugänge einzusetzen.

Im Gegensatz zu IPv4 stehen bei IPv6 genügend Adressen zur Verfügung und es ist damit zu rechnen, dass cgNAT langfristig an Bedeutung verlieren wird. Im Moment ist aber eher eine zunehmende Bedeutung aufgrund der erschöpften Reserven von IPv4-Adressen und des stark wachsenden mobilen Datenverkehrs (z. B. Smartphones, Tablets) zu beobachten.

Absatz 1 bestimmt, welche Angaben in der Antwort zu liefern sind, falls die Identifikation erfolgreich war. Falls die Identifikation nicht erfolgreich war, wird kein Ergebnis geliefert. Falls die Identifikation zu mehreren Treffern geführt hat, sind diese Datensätze zu liefern, sofern die Anzahl der Treffer den in der Anfrage angegebenen Höchstwert nicht überschreitet. Andernfalls ist lediglich die Anzahl der Treffer bekanntzugeben (Art. 18 Abs. 6).

Absatz 2 bestimmt, welche Angaben das Auskunftsgesuch enthalten muss:

- die öffentliche Quell-IP-Adresse (*Bst. a*), das heisst die gemeinsam benutzte öffentliche IP-Adresse, die im Internet als Originating IP sichtbar ist.

- falls für die Identifikation notwendig, das heisst im Falle eines NAT-Verfahrens, die öffentliche Quell-Port-Nummer (*Bst. b*), die im Internet als Originating Port sichtbar ist.

  Hinweis: Die private Quell-IP-Adresse und -Portnummer (private IP/port) sind nur der Zugangsanbieterin bekannt.

- falls für die Identifikation notwendig, das heisst im Falle eines nicht-deterministischen NAT-Verfahrens, die öffentliche IP-Adresse und die Portnummer des Ziels der Verbindung (z. B. Webserver) sowie der Typ des Transportprotokolls, z. B. TCP, UDP (*Bst. c, d und e*);

- der Zeitpunkt nach Datum und Uhrzeit (*Bst. f*). Im Auskunftsgesuch kann statt eines fixen Zeitpunkts ein Zeitintervall eingegeben werden, insbesondere um mögliche Ungenauigkeiten der Systemuhren zu kompensieren. Die Zeitangabe muss hinreichend genau und das Zeitintervall möglichst kurz sein, damit falsch-positive Treffer vermieden werden (s. Erläuterungen zu Art. 36).

Zusammengefasst sind für das Vorgehen folgende Schritte vorgesehen:

- 1. Schritt (gehört zu den Vorarbeiten und ist nicht Teil dieses Auskunftstyps): IP-History für das gesuchte Benutzerkonto bei der Betreiberin des Internet-Dienstes (Server-Seite) beschaffen, um die Verbindungsdetails der fraglichen Login-Ereignisse zu bestimmen.

- 2. Schritt: Auskunftsgesuch an die Internetzugangsanbieterin stellen (Angabe der Verbindungsdetails eines konkreten Login-Ereignisses, das im 1. Schritt bestimmt wurde), um den Teilnehmenden zu identifizieren.

- 3. Schritt (ist nicht Teil dieses Auskunftstyps): Auskunftsgesuch an die Internetzugangsanbieterin (Angabe der im 2. Schritt gefundenen Teilnehmer- bzw. Dienstidentifikatoren), um die Personendaten des Teilnehmenden abzufragen.

Details zum 1. Schritt (gehört zu den Vorarbeiten und ist nicht Teil dieses Auskunftstyps): Abfrage der sogenannten IP-History für ein bestimmtes Benutzerkonto bei der Dienstanbieterin auf der Server-Seite, das heisst am Ziel der Verbindung (Beispiele: Blog-Betreiber, Webmail, soziales Netzwerk)

Als Resultat erhält die Strafverfolgungsbehörde ein Verbindungsprotokoll mit allen Angaben zur Bestimmung der Internetzugänge, von wo aus die Zugriffe auf das gesuchte Benutzerkonto erfolgten: Quelle der Verbindung (IP-Adresse + Port), Ziel der Verbindung (IP-Adresse + Port), Zeitstempel, Typ des Protokolls. Mit Hilfe dieser Angaben kann dann im 2. Schritt die Identifikation der Benutzerschaft erfolgen.

Details zum 2. Schritt: Beispielsweise könnte eine Suche für einen mobilen Internetzugang wie folgt ablaufen. Anhand der 3 bis 6 Angaben des Auskunftsgesuchs sucht die Zugangsanbieterin in den bei ihr gespeicherten NAT-Übersetzungsdaten die private IP Adresse und Portnummer (die dem gesuchten Teilnehmenden zum gesuchten Zeitpunkt zugeordnet waren, das heisst Source IP [private IP/port]). Danach wird, anhand der gefundenen privaten IP-Adresse und Portnummer sowie des Zeitstempels, die MSISDN oder IMSI des Teilnehmenden gesucht. Die Zugangsanbieterin teilt dann den Teilnehmer- bzw. Dienstidentifikator (z. B. MSISDN, IMSI) als Ergebnis dieses Auskunftstyps mit.

Details zum 3. Schritt (ist nicht Teil dieses Auskunftstyps): Die Strafverfolgungsbehörde stellt zum Schluss ein weiteres Auskunftsgesuch (IR_4_NA), um anhand des im 2. Schritt gefundenen Teilnehmer- bzw. Dienstidentifikators (z. B. MSISDN, IMSI) die entsprechenden Personendaten dieses Teilnehmenden abzufragen.

Es sind auch ähnliche Abfragen möglich, zum Beispiel bei Dual-Stack Lite (DS Lite).

Seit der Version V1.14.1 des ETSI-Standards TS 102 657, welche im März 2014 veröffentlicht wurde, gibt es eine standardisierte Datenstruktur für NAT-Daten (Annex E.3 "ASN.1 definitions for network access services").

Die technischen Herausforderungen bei der Speicherung und Abfrage von NAT-Übersetzungsdaten bestehen darin, dass die Anbieterinnen erhebliche Datenmengen speichern und die Effizienz der Suchvorgänge sicherstellen müssen. Die vielen unterschiedlichen IP-Verbindungen, die gleichzeitig über den NAT-Router laufen, werden anhand der oben beschriebenen Parameter unterschieden. Ein einzelner Benutzer benutzt dabei in der Regel Dutzende bis Hunderte von IP-Verbindungen gleichzeitig. Die Quell-Portnummern und die übersetzten Portnummern werden zyklisch wieder frei gegeben und neu zugeteilt. Beispielsweise wird bei Smartphones die Internet-Verbindung bei Nichtgebrauch abgebaut, um Batteriestrom zu sparen. Daher bekommt das Smartphone beim Neuaufbau der Internetverbindung eine neue (private) IP-Adresse zugeteilt. Daraus ergibt sich ein enorm dynamischer Ablauf, der erhebliche Datenmengen generiert. Aktuell geht man in grossen Schweizer Mobilnetzen von etwa einer Milliarde NAT-Übersetzungsvorgängen pro Tag aus.

Die Strafverfolgungsbehörden müssen sich bewusst sein, dass es bei diesem Auskunftstyp möglich ist, dass es zu keinem Ergebnis beziehungsweise zu mehrdeutigen Ergebnissen kommen kann, insbesondere wenn nicht alle erforderlichen Parameter in der Anfrage angegeben wurden. Die Treffergenauigkeit kann beispielsweise durch die Korrelation mehrerer Anfragen erhöht werden. Die Speicherung der NAT-Übersetzungsdaten durch die Anbieterinnen löst nicht allein das Problem der Teilnehmeridentifikation im Internet. Häufig speichern die Zielserver keine Quell-Portnummern und keine exakten Zeitstempel. Aufgrund des hochdynamischen Ablaufs des NAT werden aber möglichst vollständige und präzise Angaben benötigt, um falschpositive Ergebnisse zu vermeiden.

Zum Schluss ein Hinweis: Bei diesem Auskunftstyp muss aufgrund der dynamischen Zuteilung von Adressierungselementen in den aufbewahrten Randdaten gesucht werden, wem das gesuchte Adressierungselement zum fraglichen Zeitpunkt zugeteilt war. Diese Suche muss möglicherweise in mehreren Schritten erfolgen, indem man die bekannte Spur weiterverfolgt bis zum Ursprung beziehungsweise Ziel der Verbindung. Das ist aber keine rückwirkende Überwachung, da die gesuchte Verbindung bereits bekannt ist und nur der wirkliche Ursprung beziehungsweise das wirkliche Ziel der Verbindung herausgefunden werden soll. Die Daten über die Zuteilung von dynamischen IP-Adressen und, falls für die Identifikation der Benutzerschaft notwendig, über die Übersetzung von IP-Adressen und Portnummern müssen durch die Zugangsanbieterin nur während 6 Monaten gespeichert werden (Art. 21 Abs. 2 2. Satz und 22 Abs. 2 2. Satz und Abs. 4 BÜPF sowie Art. 21 Abs. 2). FDA mit

reduzierten Überwachungspflichten gemäss Artikel 51 sind von der Pflicht zur Randdatenaufbewahrung befreit (s. auch die Erläuterungen zu Art. 18 Abs. 4).

Art. 39 Auskunftstyp IR_9_NAT: Auskünfte über NAT-Übersetzungsvorgänge

Dieser Auskunftstyp ist neu und dient der Identifikation der Benutzerschaft bei Straftaten über das Internet gemäss Artikel 22 BÜPF. Er basiert auf dem ETSI-Standard TS 102 657.

Hinweis: Der NAT-Übersetzungsvorgang wird im Folgenden als *NAT-Operation* bezeichnet. Es gibt zwei Abfragemöglichkeiten "vor" und "nach" der NAT-Operation. Diese sind zeitlich und aus Sicht der angefragten Mitwirkungspflichtigen zu verstehen):

- Abfragemöglichkeit 1

  Es sind die Angaben **nach** der NAT-Operation bekannt, gesucht sind die Angaben **vor** der NAT-Operation, z. B. bekannt ist die öffentliche Quell-IP-Adresse und Portnummer nach der NAT-Operation), gesucht ist die IP-Adresse vor der NAT-Operation.
  Analog zum Artikel 38 Absatz 2 muss das Auskunftsgesuch über NAT-Operationen folgende Angaben enthalten (*Abs. 2*):

  - die Quell-IP-Adresse und Port-Nummer nach der NAT-Operation (*Bst. a und b*), z. B. die gemeinsam benutzte öffentliche IP-Adresse sowie die Portnummer, die im Internet als sog. "Source IP/port" sichtbar sind;
  - den Typ des Transportprotokolls, z. B. TCP (*Bst. e*);
  - den Zeitpunkt der NAT-Operation nach Datum und Uhrzeit (*Bst. f*).
  - Falls für die Identifikation notwendig (hängt vom NAT-Verfahren ab), muss das Auskunftsgesuch die öffentliche IP-Adresse und Portnummer (*Bst. c und d*) des Ziels der Verbindung enthalten.

- Abfragemöglichkeit 2

  Es sind die Angaben **vor** der NAT-Operation bekannt, gesucht sind die Angaben **nach** der NAT-Operation - bekannt ist die IP-Adresse **vor** der NAT-Operation (z. B. private IP-Adresse), gesucht ist die IP-Adresse **nach** der NAT-Operation (z. B. öffentliche Quell-IP-Adresse)
  Analog zum Artikel 37 Absatz 2 muss das Auskunftsgesuch über NAT-Operationen folgende Angaben enthalten (*Abs. 2*):

  - Die Quell-IP-Adresse und Port-Nummer vor der NAT-Operation (*Bst. a und b*), z. B. die private IP-Adresse der Internetzugangsanbieterin sowie die Portnummer;
  - den Typ des Transportprotokolls, z. B. TCP (*Bst. e*);
  - den Zeitpunkt der NAT-Operation nach Datum und Uhrzeit (*Bst. f*).
  - Falls für die Identifikation notwendig (hängt vom NAT-Verfahren ab), muss das Auskunftsgesuch die öffentliche IP-Adresse und Portnummer (*Bst. c und d*) des Ziels der Verbindung enthalten.

Beispiel zu Abfragemöglichkeit 1: Wenn der Auskunftstyp IR_8_IP (NAT) gemäss Artikel 38 nicht zum Erfolg führt, muss die Quell-IP-Adresse möglicherweise

weiter rückverfolgt werden, um letztendlich die Benutzerschaft zu identifizieren. Dieser Prozess wird als "Backtracking" (Rückverfolgung) bezeichnet. Das "Backtracking" ist nur möglich, wenn jede der beteiligten Mitwirkungspflichtigen präzise und vollständig alle für die Identifikation notwendigen Informationen ihrer NAT-Übersetzungen speichert. Welche Informationen dies im Einzelnen sind, hängt von den Verfahren ab, welche die Mitwirkungspflichtige verwendet. Beim Backtracking ist auch ein mehrstufiges Verfahren möglich (von NAT zu NAT), das heisst Anfragen an alle Mitwirkungspflichtigen, die für die gesuchte Internet-Verbindung eine NAT-Übersetzung durchgeführt haben.

Beispiel zu Abfragemöglichkeit 2: Im Rahmen einer Echtzeitüberwachung des Netzzugangs wird festgestellt, dass die überwachte Person einen bestimmten abgeleiteten Kommunikationsdienst benutzt. Die Daten werden jedoch verschlüsselt übertragen, so dass der Benutzeridentifikator des abgeleiteten Kommunikationsdienstes bei der Netzzugangsüberwachung nicht sichtbar ist. Die Strafverfolgungsbehörde möchte nun den Benutzeridentifikator herausfinden. Bei der Anbieterin des abgeleiteten Kommunikationsdienstes ist jedoch aufgrund der NAT-Operation der Zugangsanbieterin eine andere (öffentliche) Quell-IP-Adresse sichtbar, als die der überwachten Person zugeteilte (private) IP-Adresse, welche der Strafverfolgungsbehörde aufgrund der Randdaten der Echtzeitüberwachung bekannt ist. Um den fraglichen Zugriff bei der Anbieterin des abgeleiteten Kommunikationsdienstes identifizieren zu können, kann die gesuchte öffentliche Quell-IP-Adresse und die Quell-Portnummer unter Angabe der bekannten IP-Verbindungsdaten bei der Zugangsanbieterin mittels dieses Auskunftstyps abgefragt werden.

5. Abschnitt: Auskunftstypen für Anwendungen

Art. 40 Auskunftstyp IR_10_TEL: Auskünfte über Teilnehmende von Telefonie- und Multimediadiensten

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Teilnehmende von Telefonie- und Multimediadiensten. Dieser Auskunftstyp entspricht im Prinzip den bisherigen Auskünften A0 und teilweise A1 (Abs. 2 Bst. j und k). Neu sind Abfragen nach der Unternehmens-Identifikationsnummer (Abs. 2 Bst. g), dem Teilnehmeridentifikator (Abs. 2 Bst. h) und den Identifikatoren (Abs. 2 Bst. i).

Zu den Telefonie- und Multimediadiensten zählen insbesondere die klassischen analogen und digitalen Telefoniedienste im Festnetz (z. B. POTS, ISDN), die mobilen Telefoniedienste inklusive SMS und Voice Mail (z. B. GSM, UMTS), die Internet-Telefonie (z. B. VoIP), die Multimedia-Telefoniedienste des IMS (z. B. VoLTE, VoWLAN, Präsenz, RCS), die Videotelefonie und die Konferenzschaltungen.

Dieser Auskunftstyp basiert auf dem ETSI-Standard TS 102 657 und kombiniert die allgemeinen Teilnehmerinformationen (generic subscriber info) mit den wichtigsten Angaben zu den Telefonie- und Multimediadiensten des Teilnehmenden. Weitere spezifische Angaben über Telefonie- und

Multimediadienste können über den Auskunftstyp IR_12_TEL (Art. 41) abgefragt werden.

Dieser Auskunftstyp gilt sowohl für Abonnements- und Prepaid-Verhältnisse als auch für Gratisangebote. Er ist analog zu Artikel 35 aufgebaut, weshalb die dortigen Erläuterungen auch für diese Bestimmung gelten.

Ähnlich wie bei Artikel 35 Absatz 1 hält *Absatz 1* fest, welche Angaben im Falle einer Auskunft über Teilnehmende von Telefonie- und Multimediadiensten zu liefern sind. Die Angaben zum Typ des Dienstes (*Ziff. 4*) dienen zur näheren Beschreibung des Dienstes. Bei den Installationsadressen des Festnetzzugangs und jeweils deren Gültigkeitszeitraum (*Ziff. 5*) sind, soweit es sich um einen Telefonie - und Multimediadienst im Festnetz handelt, die bei der Anbieterin registrierten Angaben zu liefern. Da sich der Standort im Laufe der Kundenbeziehung ändern kann, ist die gesamte bekannte Historie zu liefern, jeweils mit Beginn- und End-Datum (soweit zutreffend). Bei diesen Angaben kann jedoch nicht immer garantiert werden, dass sie mit dem tatsächlichen Standort des Zugangs übereinstimmen, da der Teilnehmende bei manchen Dienstangeboten die entsprechenden Zugangsgeräte auch ohne Wissen der Anbieterin an einem anderen Standort betreiben kann.

Anzugeben hat die Anbieterin ausserdem, soweit zutreffend, die Liste beziehungsweise den Bereich der weiteren im Zusammenhang mit dem Telefonie- oder Multimediadiensten registrierten Adressierungselemente (*Ziff. 7*) sowie falls zutreffend, die Angaben zur vorbestimmten freien Wahl der Anbieterin für Verbindungen (*Ziff. 9*). Unter den Angaben zur vorbestimmten freien Wahl der Dienstanbieterin für Verbindungen ist der voreingestellte (pre-selected) Carrier Selection Code zu verstehen. Gemäss Artikel 9 Absatz 1 der Verordnung der Eidgenössischen Kommunikationskommission vom 17. November 1997[47] betreffend das Fernmeldegesetz müssen die Anbieterinnen öffentlicher Telefoniedienste über ein Festnetz ihren Teilnehmenden die Möglichkeit bieten, eine Anbieterin für nationale und internationale Verbindungen zu wählen, und zwar sowohl vorbestimmt als auch für jeden einzelnen Anruf. Falls die vorbestimmte Wahl der Anbieterin für nationale und internationale Verbindungen bekannt ist, hat die Anbieterin des Telefoniedienstes über ein Festnetz diese Information im Rahmen des Auskunftsgesuches mitzuteilen.

Auch *Absatz 2* hält ähnlich wie Artikel 35 Absatz 2 die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind (s. die entsprechenden Erläuterungen zu Art. 35 Abs. 2). Bei einer Suche nach Zeichenketten (*Bst. a, c, d und f*) hat die Anbieterin eine sogenannte buchstabengetreue Suche gemäss Artikel 13 Absatz 1 VD-ÜPF durchzuführen (s. Erläuterungen zu Art. 35 Abs. 2).

Bei den Anfragekriterien wird zwischen den Buchstaben h, j und k sowie Buchstabe i unterschieden. Die Buchstaben h, j und k bestimmen eindeutig bestimmte Telefonie- und Multimediadienste, dienen aber im Gegensatz zu Buchstabe i nicht zur Adressierung beim Kommunikationsaufbau. Identifikatoren wie IMSI oder IMPI dienen zur Identifizierung des Teilnehmenden gegenüber dem Netz und werden von den Anbieterinnen hochvertraulich behandelt.

47 SR **784.101.112**

Da eine Anbieterin gestützt auf Artikel 23 der Verordnung vom 6. Oktober 1997[48] über die Adressierungselemente im Fernmeldebereich (AEFV) Telefonnummern aus einem ihr zugeteilten Nummernblock weiter zuteilen kann (sog. untergeordnete Zuteilung einer Telefonnummer), sind bei dieser Anbieterin in der Regel für die untergeordnet zugeteilten Telefonnummern keine aktuellen Teilnehmerdaten vorhanden. In diesem Fall hat diese Anbieterin in ihrer Antwort die untergeordnete Zuteilung sowie den Namen und die Kontaktdaten (Adresse, Telefonnummer) derjenigen Anbieterin anzugeben, an welche die abgefragte Telefonnummer weiter zugeteilt wurde.

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

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Telefonie- und Multimediadienste. Dieser Auskunftstyp entspricht im Prinzip der bisherigen Auskunft A1 (technische Daten). Der Begriff *Telefonie- und Multimediadienste* wird bei Artikel 40 erläutert.

Absatz 1 hält ähnlich wie Artikel 36 Absatz 1 fest, welche Angaben im Falle einer Auskunft über Telefonie- und Multimediadienste zu liefern sind. Betreffend die Liste der Geräteidentifikatoren (*Bst. d*) wird auf die Erläuterungen zu Artikel 36 Absatz 1 Buchstabe d verwiesen.

Der in der Antwort angegebene Gültigkeitszeitraum bezieht sich auf die drei Parameter gemäss den Buchstaben b (Adressierungselement), c (IMSI) und e (SIM-Nummer) von Absatz 1 gemeinsam. Wie bereits ausgeführt, bezieht sich dieser Gültigkeitszeitraum nicht auf die Geräteidentifikatoren. Wenn sich einer der drei vorgenannten Parameter innerhalb des in der Anfrage angegebenen Zeitraums geändert hat, hat die Mitwirkungspflichtige dem jeweiligen Stand der Informationen entsprechend mehrere Datensätze zu liefern. Da die PUK-Codes fest mit einer SIM-Karte verknüpft sind, muss für den Antwortparameter gemäss Absatz 1 Buchstabe f (PUK-Code) kein Gültigkeitszeitraum angegeben werden. Dessen Gültigkeit ergibt sich direkt aus der Gültigkeit der SIM-Nummer (*Abs. 1 Bst. e*).

Auch *Absatz 2* hält ähnlich wie Artikel 36 Absatz 2 die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind (s. die Erläuterungen zu Art. 36 Abs. 2).

Bei den Anfragekriterien wird zwischen Adressierungselementen (*Bst. a*) und Identifikatoren (*Bst. b*, *c* und *e*) unterschieden.

Art. 42 Auskunftstyp IR_13_EMAIL: Auskünfte über Teilnehmende von E-Mail- Diensten

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Teilnehmende von E-Mail-Diensten. Dieser Auskunftstyp entspricht im Prinzip den bisherigen Auskünften A0 und teilweise A1.

Dieser Auskunftstyp ist analog zu Artikel 40 aufgebaut, weshalb die dortigen Erläuterungen auch für diese Bestimmung gelten. *Absatz 1* hält fest, welche

[48] SR **784.104**

Angaben im Falle einer Auskunft über Teilnehmende von E-Mail-Diensten zu liefern sind.

Unter den anzugebenden weiteren Adressierungselementen, die zum betreffenden Dienst gehören (*Bst. c Ziff. 4*) sind zum Beispiel Alias-Adressen zu verstehen. Alias-Adressen sind zusätzliche E-Mail-Adressen, die zum selben E-Mail-Postfach gehören. Der Teilnehmende kann diese beliebig einrichten, ändern oder löschen. Deren maximale Anzahl und Aufbau werden von der E-Mail-Anbieterin vorgegeben. Die Alias-Adressen sind mit dem betreffenden E-Mail-Postfach verknüpft. An eine Alias-Adresse gesendete E-Mails werden in das gleiche E-Mail-Postfach der zugehörigen Haupt-E-Mail-Adresse des Teilnehmenden zugestellt.

Falls zutreffend sind gemäss *Ziffer 5* alle E-Mail-Adressen anzugeben, an welche die an die angefragte E-Mail-Adresse adressierten Nachrichten automatisch weitergeleitet werden, zum Beispiel im Falle einer Mailingliste. Die Mailingliste ist eine Liste von E-Mail-Adressen und wird auch als Verteilerliste oder Verteilergruppe bezeichnet. Die Mailingliste besitzt selbst eine E-Mail-Adresse. Die Nachrichten, die an die Adresse der Mailingliste geschickt werden, werden an die E-Mail-Adressen ihrer Mitglieder weitergeleitet. In diesem Beispiel sind die E-Mail-Adressen der Mitglieder der Mailingliste anzugeben.

Unter den weiteren Adressierungselementen gemäss *Buchstabe d* sind andere E-Mail-Adressen oder Telefonnummern zu verstehen, die mit dem betreffenden Dienst an und für sich nichts zu tun haben. Diese alternativen Adressierungselemente werden zum Beispiel verwendet, um das Passwort zurückzusetzen oder Sicherheitsmeldungen an den Teilnehmenden zu senden.

Absatz 2 hält ähnlich wie Artikel 40 Absatz 2 die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind (s. die entsprechenden Erläuterungen zu Art. 40 Abs. 2). Bei einer Suche nach Zeichenketten (*Bst. a, c, d und f*) hat die Anbieterin eine sogenannte buchstabengetreue Suche gemäss Artikel 13 Absatz 1 VD-ÜPF durchzuführen (s. Erläuterungen zu Artikel 35 Absatz 2).

Art. 43 Auskunftstyp IR_15_COM: Auskünfte über Teilnehmende von anderen Fernmelde- oder abgeleiteten Kommunikationsdiensten

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Teilnehmende von anderen Fernmelde- oder abgeleiteten Kommunikationsdiensten. Auch dieser Auskunftstyp entspricht im Prinzip den bisherigen Auskünften A0 und teilweise A1, wird aber neu für diese Kategorie von Diensten eingeführt. Durch diese Bestimmung sollen alle Fernmelde- oder abgeleiteten Kommunikationsdienste erfasst werden können, die zwar bereits in Betrieb sind, für welche die entsprechenden ETSI-Standards jedoch erst in Bearbeitung stehen. Die Bestimmung soll auch als Auffangtatbestand für alle weiteren, durch den technischen Fortschritt zu erwartenden Dienste dienen. Als Beispiel können die Kommunikationsdienste in sozialen Netzen, Cloud- und Proxy-Dienste aufgeführt werden. Cloud-Dienste sind abgeleitete Kommunikationsdienste wie verteilte Speicherdienste und Applikationen, die über das Internet angeboten werden. Diese sind online verfügbar und je nach Ressourcenbedarf in verteilten Rechenzentren beherbergt. Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen. Proxy-

Dienste sind daher für die Identifikation der Benutzerschaft bei Straftaten über das Internet relevant.

Ebenso in diese Kategorie gehören die Mitteilungsdienste, welche eigenständige (d. h. unabhängig von Telefonie- und Multimediadiensten angebotene) hauptsächlich asynchrone Dienste zur Übermittlung von Mitteilungen oder Nachrichten sind. Dazu gehören unter anderem Instant Messaging, IMS Messaging, Messaging Applikationen (Apps) und SMS von Drittanbieterinnen (d.h. SMS-Dienste, die nicht von der FDA des Teilnehmenden erbracht werden). Diese Dienste können auch erweiterte Zusatzfunktionen enthalten wie Multimediakommunikation, Dateiübertragung und Präsenzinformationen (z. B. der Teilnehmende kann den aktuellen Status und eventuell den Standort der anderen Teilnehmenden sehen).

Dieser Artikel ist gleich aufgebaut wie die Artikel 40-42. Aus diesem Grund kann auf die Erläuterungen zu letzteren Bestimmungen verwiesen werden.

Absatz 1 hält fest, welche Angaben im Falle einer Auskunft über Teilnehmende von anderen Fernmelde- oder abgeleiteten Kommunikationsdiensten zu liefern sind. Der Identifikator gemäss Buchstabe c Ziffer 5 kann zum Beispiel ein eindeutiger applikations- und gerätespezifischer Identifikator sein, der für Benachrichtigungen einer App benutzt wird. Mit diesem applikations- und gerätespezifischen Identifikator wird sichergestellt, dass die Benachrichtigung einer bestimmten App an ein bestimmtes Gerät geschickt wird (z. B. Device Token des Apple Push Notification service, Registration Identifier des Google Cloud Messaging, Channel URI des Windows Push Notification Service). Dieser Parameter kann für die Lieferung eines eindeutigen applikations- und gerätespezifischen Identifikators in der Antwort genutzt werden.

Absatz 2 hält, ähnlich wie in Artikel 40-42, die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind (s. die entsprechenden Erläuterungen zu Art. 40 Abs. 2). Bei einer Suche nach Zeichenketten (*Bst. a, c, d und f*) hat die Anbieterin eine sogenannte buchstabengetreue Suche gemäss Artikel 13 Absatz 1 VD-ÜPF durchzuführen (s. Erläuterungen zu Artikel 35 Absatz 2). Der Parameter gemäss Buchstabe i kann zum Beispiel für ein Auskunftsgesuch mittels eindeutigem applikations- und gerätespezifischem Identifikator genutzt werden.

6. Abschnitt: Weitere Auskunftstypen

Art. 44 Auskunftstyp IR_17_PAY: Auskünfte über die Zahlungsweise der Teilnehmenden von Fernmelde- und abgeleiteten Kommunikationsdiensten

Die Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über die Zahlungsweise der Teilnehmenden von Fernmelde- und abgeleiteten Kommunikationsdiensten. Da sich die Zahlungsweise nicht wesentlich zwischen den einzelnen Dienstkategorien unterscheidet, werden mit diesem Auskunftstyp alle Dienstkategorien abgedeckt. Dieser Auskunftstyp basiert auf dem ETSI-Parameter PaymentDetails.

Für die bisherige Auskunft A1 (technische Daten) über verwendete Aufladecodes (auch Rubbelcodes oder Scratch Codes genannt) für Prepaid-Dienste gibt es noch keinen geeigneten ETSI-Parameter. Neu erfolgt eine Ausweitung der mit diesem Auskunftstyp einholbaren Auskünfte auf alle Arten von Zahlungsweisen im Zusammenhang mit Fernmelde- beziehungsweise abgeleiteten Kommunikationsdiensten, unabhängig davon, ob es sich um Prepaid- oder abonnierte Dienste handelt.

Absatz 1 hält fest, welche Angaben zu liefern sind.

Absatz 2 hält fest, dass nur diejenigen Daten geliefert werden müssen, die bei den Anbieterinnen vorhanden sind. Beispielsweise sind bei Gratisdiensten wie E-Mail keine Informationen über die Zahlungsweise nötig und demzufolge nicht vorhanden.

Absatz 3 hält die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind.

Art. 45 Auskunftstyp IR_18_ID: Ausweiskopie

Welche Angaben zur Person im Bereich Mobilfunk sowohl beim Verkauf von Prepaid-Karten als auch bei Abonnementsabschlüssen und bei Gratisangeboten zu erfassen sind, wird in Artikel 20 geregelt. Damit die Korrektheit der erfassten Angaben gewährleistet werden kann sowie um Falschregistrierungen vorzubeugen, wird unter anderem verlangt, dass die betreffende Mitwirkungspflichtige auch eine elektronische Kopie des Ausweises des betreffenden Teilnehmenden hinterlegt. Wie die betreffende Mitwirkungspflichtige die elektronische Kopie hinterlegt, wird nicht vorgeschrieben. Vorausgesetzt wird lediglich, dass die hinterlegte elektronische Kopie des Ausweises gut lesbar und die Mitwirkungspflichtige in der Lage ist, diese auf Anfrage hin zu liefern.

Mit diesem Auskunftstyp können die berechtigten Behörden die gespeicherte Ausweiskopie zu einem bestimmten Teilnehmenden beziehungsweise Dienst abrufen. Die berechtigte Behörde hat dabei im Auskunftsgesuch zu präzisieren, auf welchen Zeitpunkt und auf welchen eindeutigen Teilnehmer- oder Dienstidentifikator sich die Anfrage bezieht (*Abs. 2*). Die Ausweiskopie ist auf elektronischem Wege zu liefern. Bei Netzzugangsdiensten kann die Anfrage auch anhand einer Gerätenummer erfolgen. Einen direkten Zusammenhang von Geräteidentifikator und Ausweiskopie besteht eigentlich nur dann, wenn das Gerät zusammen mit dem Vertragsabschluss und zeitgleicher Ausweiserfassung bezogen wurde. Ferner besteht immer die Möglichkeit der Weitergabe (z. B. Verkauf) des Gerätes an Dritte, was durch die Anbieterin nicht verfolgt werden kann.

Art. 46 Auskunftstyp IR_19_BILL: Rechnungskopie

Dieser Auskunftstyp entspricht der bisherigen Auskunft A2 (Rechnungsdaten); siehe insbesondere Art. 21 Abs. 1 Bst. d BÜPF. Die Mitwirkungspflichtige muss eine elektronische Kopie der vorhandenen Rechnungsunterlagen des Teilnehmenden liefern. Wichtig ist, dass dabei keinerlei Randdaten mitgeliefert werden. Beispielsweise dürfen keine Verbindungen auf der Rechnungskopie erscheinen. Es genügt zum Beispiel, jeweils die erste Seite (Zusammenfassung) der Monatsrechnungen zu übermitteln, welche den Rechnungsbetrag, die Kundennummer und die Rechnungsadresse enthält. Die anfragende Behörde hat in

ihrem Auskunftsgesuch zu präzisieren, auf welchen Zeitraum und auf welchen eindeutigen Teilnehmer- oder Dienstidentifikator sich die Anfrage bezieht (*Abs. 2*).

Art. 47 Auskunftstyp IR_20_CONTRACT: Vertragskopie

Dieser Auskunftstyp entspricht der bisherigen Auskunft A2 (Vertragskopie); siehe insbesondere Art. 21 Abs. 1 Bst. d BÜPF. Im Falle einer Auskunftsanfrage ist eine elektronische Kopie der vorhandenen Vertragsunterlagen oder von vergleichbaren Aufzeichnungen zu liefern. Da Verträge sowohl schriftlich als auch mündlich abgeschlossen werden können, kann es vorkommen, dass kein schriftlicher Vertrag vorhanden ist. Durch diese Bestimmung wird keine Verpflichtung für die Mitwirkungspflichtigen eingeführt, nur noch schriftliche Verträge abschliessen zu müssen. Sollte kein schriftlicher Vertrag vorhanden sein, genügt es, dass die Mitwirkungspflichtige zum Beispiel eine Bildschirmkopie aus ihrem System liefert, welche über die Vertragsbeziehung Auskunft gibt. Die berechtigte Behörde hat in ihrem Auskunftsgesuch zu präzisieren, auf welchen Zeitpunkt und auf welchen eindeutigen Teilnehmer- oder Dienstidentifikator sich die Anfrage bezieht (*Abs. 2*). Bei Netzzugangsdiensten kann die Anfrage auch anhand einer Gerätenummer erfolgen. Einen direkten Zusammenhang von Geräteidentifikator und Ausweiskopie besteht eigentlich nur dann, wenn das Gerät zusammen mit dem Vertragsabschluss und zeitgleicher Ausweiserfassung bezogen wurde. Ferner besteht immer die Möglichkeit der Weitergabe (z. B. Verkauf) des Gerätes an Dritte, was durch die Anbieterin nicht verfolgt werden kann.

Art. 48 Auskunftstyp IR_21_TECH: Technische Daten

Dieser Artikel hält fest, dass die Mitwirkungspflichtigen die technischen Daten von Fernmeldesystemen und Netzelementen zu liefern haben (s. insbesondere Art. 21 Abs. 1 Bst. d BÜPF). Sie haben diese Daten 6 Monate rückwirkend aufzubewahren. Es wäre jedoch denkbar, dass beispielsweise zu einer ausgeführten rückwirkenden Überwachung zu einem späteren Zeitpunkt noch Rückfragen zu Daten der Abdeckung einer Antenne gestellt werden, die länger als 6 Monate zurück liegen. In diesem Fall müssten die Mitwirkungspflichtigen diese Daten liefern, sofern diese noch vorhanden sind.

Dieser Auskunftstyp entspricht der bisherigen Auskunft A3. In erster Linie geht es dabei um die Standortangaben von Mobilfunkantennen und öffentlichen WLAN-Zugangspunkten. Die Übermittlung weiterer Angaben wie der Typ der Mobilfunktechnologie und die Frequenzen ist nach heutigem Stand im ETSI-Standard nicht enthalten. Es ist vorgesehen, diese im Rahmen einer zukünftigen Teilrevision dieser Verordnung hinzuzufügen, sobald die Voraussetzungen im ETSI-Standard geschaffen wurden. Der proprietäre Standard für die Übermittlung der Ergebnisse einer manuellen Notsuche EP_35_PAGING enthält diese Angaben bereits.

Was die Standortangaben von Mobilfunkzellen und WLAN-Zugangspunkten umfasst, regelt *Absatz 2* näher. Die Angaben gemäss *Buchstabe b-d* sind nur zu liefern, sofern solche vorhanden sind. Das Feld Azimuth (Hauptstrahlungsrichtung) ist im ETSI-Standard vorhanden. Es kann aber nur sinnvoll genutzt werden, wenn eine solche tatsächlich existiert, daher «gegebenenfalls». Für die Notsuche wurde ein besonderer Mechanismus entwickelt, der die Übertragung von Attributen wie

«omnidirectional» zulässt. Dieser Mechanismus steht aber hier nicht zur Verfügung.

Absatz 3 hält die einzelnen Anfragekriterien für diesen Auskunftstyp fest und schreibt vor, dass das Auskunftsgesuch mindestens eines der erwähnten Kriterien enthalten muss. Zudem hat die anordnende Behörde in ihrem Auskunftsgesuch zu präzisieren, auf welchen Zeitraum sich die Anfrage bezieht. Bei Anfragen anhand der geografischen Koordinaten (*Bst. a*) sind diese mit hinreichender Genauigkeit anzugeben und beziehen sich auf genau einen Standort. Die Anbieterin hat die technischen Daten zu allen Netzelementen zu liefern, die sich in einem Radius von 50 m um den angefragten Standort herum befinden. Mit diesem Toleranzbereich wird sichergestellt, dass das gesuchte Netzelement auch bei einer Suche über sehr präzise geografische Koordinaten gefunden werden kann. Die Anbieterin muss jedoch keine Abdeckungsanalyse für die in der Anfrage angegebenen geografischen Koordinaten durchführen. Für Abdeckungsanalysen dient der Überwachungstyp AS_32_PREP_COV (Art. 64).

7. Abschnitt: Allgemeine Bestimmungen für die Überwachung des Fernmeldeverkehrs

Art. 49 Anordnung zur Überwachung des Fernmeldeverkehrs

Diese Bestimmung entspricht im Wesentlichen dem Artikel 15 der VÜPF vom 31. Oktober 2001[49] und regelt den Inhalt der Überwachungsanordnung im Falle einer Überwachung des Fernmeldeverkehrs (für den Postverkehr, s. oben die Erläuterungen zu Art. 15). Mit Ausnahme der Zugriffsrechte kann eine bereits quittierte Überwachungsanordnung nicht mehr geändert werden. Wesentliche Änderungen einer Überwachungsanordnung wie Überwachungstyp oder zu überwachenden Identifikator (Target-ID) erfordern eine neue Überwachungsanordnung. Die Neuanordnung unterliegt den üblichen Gebühren und Entschädigungen.

Absatz 1 führt abschliessend diejenigen Angaben auf, welche die Überwachungsanordnung enthalten muss.

Buchstabe a: Der Dienst ÜPF prüft formell, ob diese Behörde zur Anordnung dieser Überwachung berechtigt ist beziehungsweise bei einer Überwachung des NDB, ob sie nach den Artikeln 29-31 NDG genehmigt und freigegeben wurde (Art. 16 Bst. a Ziff. 2 BÜPF).

Buchstabe b: Gemäss diesen Angaben erteilt der Dienst ÜPF den aufgeführten Personen die Zugriffsrechte im Verarbeitungssystem zu den Überwachungsdaten dieser Überwachung.

Buchstabe c: Falls vorhanden, dienen diese Angaben zur Kontrolle bei der FDA beziehungsweise der Anbieterin abgeleiteter Kommunikationsdienste, ob die zu überwachende Anwendung beziehungsweise der zu überwachende Internetzugang mit dieser Person in Zusammenhang stehen.

49 SR **780.11**

Buchstabe d: Die Referenznummer und der Fallname ist für die korrekte Erfassung im Verarbeitungssystem notwendig.

Buchstabe e: Der Dienst ÜPF prüft formell, ob der Straftatbestand die Anordnung dieser Überwachung gemäss Artikel 269 StPO (Echtzeitüberwachungen) oder gemäss Artikel 273 StPO beziehungsweise Artikel 70d MStP (rückwirkende Überwachungen) erlaubt.

Buchstabe f: Die anordnende Behörde teilt dem Dienst ÜPF den Namen der Mitwirkungspflichtigen mit, welche die Überwachung durchzuführen hat.

Unter *Buchstabe g* sind die angeordneten Überwachungstypen aufgeführt. Es können sowohl standardisierte als auch nicht-standardisierte Überwachungstypen angeordnet werden. Bei Unklarheiten, Widersprüchen oder zu erwartenden hohen Gebühren nimmt der Dienst ÜPF Rücksprache mit der anordnenden Behörde.

Buchstabe h: Die anordnende Behörde teilt dem Dienst ÜPF die zu überwachenden Identifikatoren mit. Bei Unklarheiten nimmt der Dienst ÜPF Rücksprache mit der anordnenden Behörde.

Buchstabe i: Falls die zu überwachende Person in rascher Folge den Fernmeldeanschluss wechselt, kann das Zwangsmassnahmengericht gemäss Artikel 272 Abs. 2 StPO mittels Rahmenbewilligung die Überwachung aller identifizierten Anschlüsse bewilligen, über welche die zu überwachende Person ihren Fernmeldeverkehr abwickelt, ohne dass jedes Mal eine Genehmigung im Einzelfall nötig ist. Der Antrag auf Rahmenbewilligung ist der Überwachungsanordnung beizulegen.

Buchstabe j: Die anordnende Behörde muss angeben, in welchem Zeitraum die Überwachung durchgeführt werden soll. Es sind hierbei die geltenden Fristen zu berücksichtigen. So können Echtzeitüberwachungen lediglich für maximal drei Monate in die Zukunft und rückwirkende Überwachungen lediglich für maximal sechs Monate in die Vergangenheit angeordnet werden.

Für die *Buchstaben k* und *l*, siehe die Erläuterungen zu Artikel 5. Buchstabe k ist die Kennzeichnung, dass diese Überwachung Personen betrifft, die einem Amts- oder Berufsgeheimnis gemäss Artikel 271 StPO oder 70b MStP wie Rechtsanwälte und Ärzte unterstehen. Der Dienst ÜPF hat für diese Überwachung die Triage der Aufzeichnung der erhaltenen Daten während einer Überwachung einer dem Amts- oder Berufsgeheimnis unterstellten Person vorzubereiten und allenfalls die Vorkehren gemäss Buchstabe l umzusetzen.

Absatz 2 bezieht sich auf Überwachungen, für deren Durchführung weitere technische Angaben erforderlich sind, beispielsweise weil der Überwachungstyp nicht standardisiert ist oder weil die Ausleitung der Überwachungsdaten nicht auf das Verarbeitungssystem des Dienstes ÜPF erfolgt.

Art. 50 Überwachungspflichten

Absatz 1 definiert den Kreis der Mitwirkungspflichtigen, die mit Überwachungen des Fernmeldeverkehrs beauftragt werden können. Einen Auftrag zur aktiven Überwachung im Bereich des Fernmeldeverkehrs können wie bisher die Anbieterinnen von Fernmeldediensten sowie neu die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten gemäss Artikel 52 erhalten. Neu wird in der Verordnung auch festgehalten, dass Anbieterinnen von Fernmeldediensten mit reduzierten Überwachungspflichten

nicht Adressat eines solchen Überwachungsauftrages sein können. Es handelt sich dabei um die Überwachungspflichten gemäss dem 3. Kapitel Abschnitt 8-12. Nach der Bestimmung müssen die betreffenden Mitwirkungspflichtigen in der Lage sein, die erwähnten Pflichten entweder selber auszuführen oder durch einen Dritten ausführen zu lassen (Art. 32 BÜPF).

Gemäss *Absatz 2* ist die Überwachungsbereitschaft von der kommerziellen Aufnahme des Kundenbetriebes eines Dienstes an sicherzustellen. Dies bedeutet, dass das Abnahmeverfahren zur Überprüfung der Auskunfts- und Überwachungsbereitschaft vorgängig durchgeführt und erfolgreich abgeschlossen werden muss (vgl. Ausführungen zu den Art. 31-34). Test- und Pilotphasen gelten nicht als kommerzielle Aufnahme des Kundenbetriebes.

Absatz 3 weist darauf hin, dass Überwachungsaufträge sowohl innerhalb als auch ausserhalb der Normalarbeitszeiten (s. Art. 10) entgegengenommen und innerhalb der vorgegebenen Frist ausgeführt werden müssen. Die Festlegung der Fristen für die Ausführung der Überwachungsaufträge wird an das EJPD delegiert. Das EJPD regelt diese Fristen in der VD-ÜPF.

Absatz 4 regelt, in welchem Zeitraum welcher Teil des Fernmeldeverkehrs zu überwachen ist. Der Dienst ÜPF sendet der Mitwirkungspflichtigen bei Echtzeitüberwachungen einen Aktivierungsauftrag zum Beginn der Überwachung und einen Deaktivierungsauftrag zu deren Ende. Bei rückwirkenden Überwachungen wird nur ein Aktivierungsauftrag gesendet, der den Überwachungszeitraum angibt. Bei Echtzeitüberwachungsaufträgen weiss die Mitwirkungspflichtige beim Eingang des Aktivierungsauftrages noch nicht, wann die Echtzeitüberwachung enden wird. Das Ende der Überwachung wird der Mitwirkungspflichtigen erst mit dem Deaktivierungsauftrag mitgeteilt.

Die Mitwirkungspflichtige muss grundsätzlich sicherstellen, dass jeglicher von ihr kontrollierter Fernmeldeverkehr überwacht werden kann. Ausgeleitet werden muss aber nur derjenige Fernmeldeverkehr, der an den überwachten Netzzugang gerichtet ist beziehungsweise von diesem stammt oder der mit der überwachten Anwendung beziehungsweise dem überwachten Identifikator (Target-ID, z. B. Telefonnummer eines Telefoniedienstes) im Zusammenhang steht (z. B. Anrufe von oder zu dieser Telefonnummer). Der Begriff "der von ihr kontrollierte Fernmeldeverkehr" umfasst die Infrastruktur, welche die Mitwirkungspflichtige besitzt, mietet, verwaltet, ausgelagert hat (Outsourcing) oder in einem besonderen Nutzungsrecht (z. B. MVNO) vertraglich nutzt. Bei der Benutzung *ausländischer* Infrastruktur (z. B. Roaming im Ausland) ist der Fernmeldeverkehr nur insoweit zu überwachen, wie er von der Mitwirkungspflichtigen im Rahmen der bei ihr üblichen technischen Betriebsverfahren (z. B. Routing, Signalisierung) kontrolliert werden kann. Grundsätzlich sollen sich die technischen Betriebsverfahren für den überwachten Teilnehmenden (Target) beziehungsweise überwachten Dienst (Target) nicht von einem nicht-überwachten Teilnehmenden beziehungsweise Dienst unterscheiden. Bei der Benutzung fremder *inländischer* Infrastruktur, zum Beispiel nationales Roaming, Mobile Virtual Network Operator (MVNO), hat die Mitwirkungspflichtige sicherzustellen, dass der gesamte zu überwachende Fernmeldeverkehr von ihr oder von Dritten ausgeleitet wird.

Eine Mitwirkungspflichtige muss also auch in der Lage sein, Fernmeldeverkehr zu überwachen, welcher Adressierungselemente betrifft, die sie nicht vergeben hat oder die sich nicht in ihrem Netz befinden beziehungsweise nicht in ihrem Netz

eingebucht sind (z. B. Überwachung einer ausländischen Telefonnummer - s. Art. 69).

Beim Roaming gibt es zwei Szenarien.

1. Outbound Roaming: Überwachung eines eigenen Teilnehmenden der beauftragten Anbieterin, wenn dessen Endgerät als Besucher in einem fremden Netz eingebucht ist. Beim Outbound Roaming werden zwei Szenarien unterschieden:

A) fremdes Netz im Inland

B) fremdes Netz im Ausland

Die beiden Szenarien unterscheiden sich dadurch, dass im Szenario A die beauftragte Anbieterin dafür sorgen muss, dass der gesamte Fernmeldeverkehr ihrer Teilnehmenden von ihr oder von Dritten auch dann überwacht wird, wenn sie das fremde Netz im Inland benutzen.

Im Szenario B dagegen muss die beauftragte Anbieterin lediglich diejenigen Randdaten und Kommunikationsinhalte überwachen können, die sie im Rahmen der bei ihr üblichen technischen Betriebsverfahren kontrolliert und auf die sie demzufolge zugreifen kann.

2. Inbound Roaming: Überwachung eines fremden Teilnehmenden, dessen Endgerät als Besucher im Netz der beauftragten Mitwirkungspflichtigen eingebucht ist. In diesem Szenario ist die Überwachung möglich, da sich der fremde Teilnehmende im Netz der beauftragten Mitwirkungspflichtigen befindet. Aufgrund bestimmter technischer Besonderheiten kann es jedoch vorkommen, dass die Kommunikationsinhalte nur verschlüsselt ausgeleitet werden können, wenn beispielsweise die Daten verschlüsselt in einem Tunnel zwischen dem fremden Teilnehmenden und dessen Heimnetzwerk übertragen werden, dessen Verschlüsselung die beauftragte Mitwirkungspflichtige nicht angebracht hat und daher auch nicht entfernen kann. Dagegen hat beispielsweise eine ausländische Mobilfunkanbieterin, die nicht als Mitwirkungspflichtige im Sinne des Art. 2 BÜPF gilt und deren Kunden lediglich als Inbound-Roamer in einem Schweizer Netz eingebucht sind, keine Pflichten gemäss dem BÜPF.

Die übermittelten Überwachungsdaten müssen mit dem im Überwachungsauftrag bezeichneten Fernmeldeverkehr übereinstimmen. Dabei muss die Mitwirkungspflichtige den Dienst ÜPF bei Bedarf unterstützen (*Abs. 5*).

Gemäss *Absatz 6* muss die Mitwirkungspflichtige des Weiteren sicherstellen, dass, falls weitere Identifikatoren mit dem überwachten Identifikator (Target-ID) assoziiert sind, auch diese im Rahmen des Überwachungstyps überwacht werden. Die möglichen Fälle von assoziierten Identifikatoren werden nach Anhörung der Anbieterin individuell vom Dienst ÜPF festgelegt (Bsp. Alias-Email-Adresse bei einer Anbieterin von E-Mail-Diensten.

Art. 51 FDA mit reduzierten Überwachungspflichten

FDA müssen grundsätzlich in der Lage sein, die Überwachungspflichten, die durch sie angebotene Dienste betreffen, auszuführen oder durch Dritte ausführen zu lassen (Art. 32 BÜPF). Dies bedeutet für die FDA unter anderem, dass sie über die für die Fernmeldeüberwachung erforderlichen Einrichtungen verfügen müssen. Die Beschaffung der erforderlichen Einrichtungen ist mit Investitionskosten verbunden,

die nicht von allen FDA gleich gut getragen werden können. Dies wird vor allem von den kleinen und mittelgrossen FDA negativ wahrgenommen. Deshalb hat der Gesetzgeber in Artikel 26 Absatz 6 BÜPF dem Bundesrat die Kompetenz eingeräumt, FDA, die Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten, von bestimmten gesetzlichen Pflichten zu befreien. Nicht befreit werden können diese Anbieterinnen jedoch von der gesetzlichen Minimalpflicht betreffend Überwachungen, eine Überwachungsmassnahme zu dulden, von ihnen angebrachte Verschlüsselungen zu entfernen, Zugang zu ihren Anlagen zu gewähren sowie die die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person auf verlangen zu liefern (Art. 26 Abs. 2 und 6 BÜPF). Im Rahmen der Vernehmlassung wurde beantragt, in den Verordnungen den Begriff «Bildungsbereich» zu ersetzen durch «Bereich Bildung und Forschung». Diesem Anliegen wurde gefolgt.

Absatz 1 konkretisiert die einzelnen Voraussetzungen, welche bestehen müssen, damit der Dienst ÜPF eine FDA auf deren Gesuch hin mittels Verfügung als eine mit reduzierten Überwachungspflichten erklären kann. Ab dann hat die gesuchstellende FDA keine weitere als die oben beschriebene gesetzliche Minimalpflicht betreffend Überwachungen zu erfüllen. Der Dienst ÜPF kann eine FDA als eine solche mit reduzierten Überwachungspflichten erklären, wenn sie ihre Fernmeldedienste nur im Bereich Bildung und Forschung anbietet (Bst. a) oder beide der Grössen nach Buchstabe b nicht erreicht. Kommt der Dienst ÜPF nach Einsicht in die Unterlagen zum Schluss, dass die FDA die Voraussetzungen gemäss Absatz 1 erfüllt, verfügt er dies und teilt es der betreffenden FDA mit. Die Überwachungsbereitschaft entfällt mit dem Erlass der entsprechenden Verfügung. Der Dienst ÜPF hat die nötigen Schritte zu unternehmen, damit die Überwachungen weiterhin durchgeführt werden können (Art. 17 Bst. e und Art. 26 Abs. 2 Bst. b BÜPF; s. auch Kommentar zu Art. 53, Zugang zu den Anlagen).

Gemäss *Buchstabe a* sind FDA, welche ihre Dienstleistungen ausschliesslich im Bereich Bildung und Forschung anbieten, rein aufgrund der Tatsache, dass sie nur in diesem Bereich tätig sind, vom Dienst ÜPF als solche mit reduzierten Überwachungspflichten zu erklären und haben lediglich die gesetzliche Minimalpflicht zu erfüllen.

Die erste Voraussetzung gemäss *Buchstabe b Ziffer 1,* damit eine FDA als eine mit reduzierten Überwachungspflichten gelten kann, ist, dass sie in den letzten zwölf Monaten Überwachungsaufträge zu weniger als 10 verschiedenen Zielen erhalten hat. Dabei dient der 30. Juni als Stichtag. Die Vorschrift bezieht sich auf die Gesamtsumme von Echtzeit- und rückwirkenden Überwachungen. Hiermit wird ein praxiserprobtes Kriterium angewandt, nämlich jenes der Anzahl der Überwachungsaufträge. Zwar sieht Artikel 26 Absatz 6 BÜPF ein solches Kriterium nicht ausdrücklich vor. Die offene Formulierung (Wörter «kann» und «insbesondere») lässt dem Bundesrat die Freiheit, weitere objektive Kriterien auszuwählen. Die Statistik der Fernmeldeüberwachungen der letzten Jahre zeigt, dass die für die Fernmeldeüberwachung relevanten Anbieterinnen jeweils eine gewisse Anzahl von Überwachungsaufträgen generiert haben. Somit können mit einer Unterschreitung einer gewissen Anzahl von Überwachungsaufträge relativ zuverlässig den für die Fernmeldeüberwachung weniger relevanten FDA nur reduzierte Überwachungspflichten auferlegt werden. Somit kann dem Verhältnismässigkeitsprinzip besser entsprochen werden.

Zudem, gemäss *Buchstabe b Ziffer 2*, darf die FDA einen Jahresumsatz von 100 Millionen Franken in den letzten zwei aufeinander folgenden Geschäftsjahren nicht erreichen, um als FDA mit reduzierten Überwachungspflichten durch den Dienst ÜPF anerkannt zu werden. Das letzte Kriterium wird dadurch weiter eingeschränkt, dass nur der mit Fernmelde- und abgeleiteten Kommunikationsdiensten erzielte Jahresumsatz in Betracht gezogen wird.

Wir gehen davon aus, dass sich aufgrund der Anwendung der Schwellenwerte gemäss Buchstabe b die Anzahl der gemäss bisherigem Recht aktiv überwachungspflichtigen FDA von rund 600 auf etwa 20 bis 30 FDA verringern wird. Auch mit der Befreiung von bestimmten Überwachungspflichten soll die Fernmeldeüberwachung weiterhin sichergestellt sein. Die Überwachungen können auch bei FDA mit reduzierten Überwachungspflichten durchgeführt werden, da diese Anbieterinnen immer eine Duldungs- und Zusammenarbeitspflicht haben. Dazu werden sie nicht von der Pflicht befreit, die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person auf Verlangen zu liefern (Art. 26 Abs. 6 BÜPF). Der Dienst ÜPF hat die nötigen Schritte zu unternehmen, damit die Überwachungen weiterhin durchgeführt werden können (Art. 17 Bst. e BÜPF).

Für den Konzerntatbestand gemäss *Absatz 2* wird sinngemäss auf Artikel 22 Absatz 2 verwiesen. Dieser regelt den Fall, bei dem ein oder mehrere rechnungspflichtige Unternehmen von einer FDA kontrolliert werden. In diesem Fall werden die beteiligten Unternehmen und die betreffende FDA als eine Einheit betrachtet. Dadurch sollen Missbrauchsfälle verhindert werden (für weitere Ausführungen, s. Art. 22).

In *Absatz 3* wird eine Mitteilungspflicht für FDA mit reduzierten Überwachungspflichten eingeführt. Bietet eine FDA ihre Dienstleistungen nicht mehr ausschliesslich im Bereich Bildung und Forschung an (*Bst. a*) oder wird die Grösse gemäss Absatz 1 Buchstabe b Ziffer 2 zum zweiten aufeinanderfolgenden Geschäftsjahr erreicht (*Bst. b*), hat die betreffende FDA dies dem Dienst ÜPF innert drei Monaten nach Abschluss ihres Geschäftsjahres mitzuteilen und entsprechende Belege einzureichen. In der Vernehmlassung wurde bemängelt, dass auch die Pflichten der FDA mit reduzierten Überwachungspflichten nicht klar ersichtlich seien. In dieser Verordnung wird allerdings der Ansatz gewählt, wonach der Umfang der Pflichten der verschiedenen Kategorien beziehungsweise Unterkategorien von Mitwirkungspflichtigen nicht gesammelt festgelegt wird, sondern jeweils an Ort und Stelle bei der materiellen Regelung. Die Tabelle am Schluss dieses erläuternden Berichts gibt einen Überblick über die Pflichten der verschiedenen Mitwirkungspflichtigen.

Absatz 4 ermöglicht dem Dienst ÜPF weitere Daten zur Verifizierung der möglichen Über- oder Unterschreitung der Grössen gemäss Absatz 4 heranzuziehen, um über das Gesuch der FDA zu entscheiden.

Wie beim Artikel 22 Absatz 5 hat die FDA die Speicherung der für die Überwachung erforderlichen Daten innert zwei Monaten und die Überwachungsbereitschaft innert zwölf Monaten sicherzustellen, sobald der Dienst ÜPF entscheidet, dass sie nicht mehr als FDA mit reduzierten Überwachungspflichten gilt (*Abs. 5*).

Art. 52 Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten

Ähnlich wie bei den Auskunftspflichten gemäss Artikel 22 BÜPF hat der Gesetzgeber in Artikel 27 Absatz 3 BÜPF dem Bundesrat die Kompetenz eingeräumt, den Anbieterinnen abgeleiteter Kommunikationsdienste weitergehende Überwachungspflichten aufzuerlegen. Diese Kompetenz wird mit diesem Artikel umgesetzt.

Die Bestimmung ist gleich aufgebaut wie Artikel 22, der die Voraussetzungen für weitergehende Auskunftspflichten für Anbieterinnen abgeleiteter Kommunikationsdienste regelt. Einziger Unterschied zu Artikel 22 bildet die alternativ zu erfüllende Voraussetzung, dass in den letzten 12 Monaten Überwachungsaufträge zu mindestens zehn verschiedenen Zielen der Überwachung (Targets) anfielen. *Buchstabe a* nimmt das in Artikel 27 Absatz 3 BÜPF genannte Kriterium „grosse Benutzerschaft" auf. Aus Sicht der Fernmeldeüberwachung ist es sehr schwierig, die grosse Benutzerschaft *absolut* zu definieren, umso mehr, wenn es gilt, diese in Bezug auf verschiedene angebotene technische Dienste im Voraus festzulegen. Aus diesem Grund wird mit Buchstabe a ein praxiserprobtes Kriterium angewandt, nämlich jenes der Anzahl Überwachungsaufträgen. Die Statistik der Fernmeldeüberwachungen der letzten Jahre zeigt, dass die Anzahl der Überwachungsaufträge verlässlich und passend auf die Art der angebotenen Dienste zuverlässig die grosse Benutzerschaft erfasst. Gleichzeitig wird mit diesem Kriterium auch die Verhältnismässigkeit abgedeckt, indem nur Anbieterinnen erfasst werden, die auch wirklich relevant für die Fernmeldeüberwachung sind. Ansonsten ist der Regelungsgegenstand beider Bestimmungen gleich, weshalb für die weiteren Ausführungen auf die Erläuterungen beim Artikel 22 verwiesen wird. (Hinweis: Eine Unterscheidung betreffend Überwachungspflichten zwischen Echtzeit- und rückwirkenden Überwachungen ist nicht vorgesehen. Die Vorschrift bezieht sich also auf die Gesamtsumme von Echtzeit- und rückwirkenden Überwachungen.)

Bei den zu erfüllenden Pflichten handelt es sich um dieselben Pflichten, die von den Fernmeldedienstanbieterinnen zu erfüllen sind, das heisst insbesondere die Pflichten gemäss Artikel 26 Absatz 1-5 BÜPF. Sie müssen also insbesondere aktive Vorbereitungen treffen, um die standardisierten Überwachungstypen gemäss dem 3. Kapitel Abschnitte 7-12 selbst auszuführen oder durch Dritte ausführen zu lassen und die Randdaten des Fernmeldeverkehrs während sechs Monaten aufbewahren. Die für die Anbieterinnen von Fernmeldediensten geltenden Bestimmungen des BÜPF sind sinngemäss auf die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten anwendbar (Art. 27 Abs. 3 BÜPF).

Art. 53 Zugang zu den Anlagen

Bei Mitwirkungspflichtigen, die Überwachungsaufträge aufgrund der gesetzlichen Vorgaben nicht aktiv auszuführen haben (so bspw. FDA mit reduzierten Überwachungspflichten gemäss Art. 51) oder solche, die aufgrund mangelnder oder fehlender Überwachungsbereitschaft nicht in der Lage sind, einen Überwachungsauftrag auszuführen, führt der Dienst ÜPF den Überwachungsauftrag entweder selbst aus oder lässt diesen durch einen Dritten ausführen (Art. 26 Abs. 2 Bst. b BÜPF). Ausserdem führt der Dienst ÜPF oder von ihm beauftragte Dritte die nicht

standardisierten Überwachungen durch (Art. 32 Abs. 2 BÜPF). Um einen solchen Überwachungsauftrag auszuführen, muss der Dienst ÜPF beziehungsweise die von ihm beauftragten Dritten Zugang zu den Anlagen der betreffenden Mitwirkungspflichtigen haben.

Artikel 53 führt näher aus, was unter der Gewährung des Zugangs zu den Anlagen einer Mitwirkungspflichtigen zu verstehen ist. Zugang zu den Anlagen bedeutet demnach insbesondere der Zutritt, physikalische Zugang und Fernzugang zu Gebäuden, Infrastrukturen, Geräten, Leitungen, Systemen, Netzen und Diensten (Abs. 1). Die Mitwirkungspflichtige muss dem Dienst ÜPF oder den von ihm beauftragten Dritten auch ihre bestehenden Netzzugänge zu öffentlichen Fernmeldenetzen (z. B. Internetanschluss) zur Verfügung stellen (Abs. 2). Hierfür kann die Mitwirkungspflichtige dem Dienst ÜPF keine Kosten in Rechnung stellen, sondern sie hat den Netzzugang kostenlos zur Verfügung zu stellen. Sind für die Ausführung eines Überwachungsauftrages Netzzugänge zu öffentlichen Fernmeldenetzen notwendig und verfügt die Mitwirkungspflichtige nicht über solche, hat sie solche zu erstellen, soweit dies ihr zugemutet werden kann. Soweit dies für die Überwachung notwendig ist, erstellen die Mitwirkungspflichten in Absprache mit dem Dienst ÜPF oder dem von ihm beauftragten Dritten neue Netzzugänge auf Kosten des Dienstes ÜPF.

8. Abschnitt: Typen der Echtzeitüberwachung von Netzzugangsdiensten

Art. 54 Überwachungstyp RT_22_NA_IRI: Echtzeitüberwachung von Randdaten bei Netzzugangsdiensten

Die Bestimmung definiert den standardisierten Überwachungstyp Echtzeitüberwachung eines Netzzugangsdienstes (entspricht dem bisherigen Überwachungstyp PS 2). Im Gegensatz zum Artikel 55 sind im Rahmen eines Überwachungsauftrages gemäss Artikel 54 lediglich die Randdaten des Fernmeldeverkehrs auszuleiten. Dieser Überwachungstyp kommt nur bei mobilen Internetzugängen zum Einsatz (*Abs. 1*), um die Standortinformationen in Echtzeit zu erhalten.

Im Rahmen dieses Überwachungstyps werden generell keine Randdaten von Anwendungen erfasst. Wenn beispielsweise über den überwachten Netzzugang eine Anwendung wie VoIP benutzt wird, werden die Randdaten der Anwendung mit dem hier definierten Überwachungstyp nicht ausgeleitet. Für die Überwachung von Anwendungen sind entsprechende Überwachungstypen vorgesehen. Als weiteres Beispiel können die MMS-Mitteilungen aufgeführt werden. So werden im Rahmen dieses Überwachungstyps die MMS-spezifischen Randdaten (MMS ist eine Anwendung) nicht ausgeleitet, sondern nur die Randdaten des Netzzugangs.

Absatz 2 hält fest, welche Randdaten des Fernmeldeverkehrs, der über den überwachten Netzzugangsdienst gesendet oder empfangen wird, in Echtzeit zu übermitteln sind. Mit den in *Absatz 1 Buchstabe g* aufgeführten "technischen Änderungen" sind Ereignisse gemeint, welche die technischen Eigenschaften des überwachten Netzzugangs verändern oder die dessen Mobility Management

betreffen, so zum Beispiel Änderungen des Trägerdienstes (Bearer Modification) oder Location Update.

Absatz 3 regelt näher, was die Standortangaben gemäss Absatz 2 Buchstabe h umfassen. Die Mitwirkungspflichtige hat dabei für die Übermittlung der Standortangaben die Wahl zwischen drei verschiedenen Varianten. Sie hat bei vom Netzwerk bestimmten Standortangaben einen entsprechenden Vermerk anzubringen, da Standortangaben des Netzwerkes geprüft und damit zuverlässiger sind als ungeprüfte, die vom Endgerät oder von einer Applikation stammen könnten.

Gemäss *Buchstabe a* hat die Mitwirkungspflichtige unter anderem die Hauptstrahlungsrichtung der Zelle mitzuteilen. Die Hauptstrahlungsrichtung ist jedoch nur mitzuteilen, wenn sie vorhanden und eindeutig ist. So darf beispielsweise bei Antennen mit mehreren Sektoren nicht ein Mittelwert für die Hauptstrahlungsrichtung gebildet werden, sondern es müssen, falls jeder Sektor einen eigenen Identifikator (z. B. Cell ID) hat, die Hauptstrahlungsrichtungen jedes Sektors mitgeteilt werden. Bei einer einfachen Zelle beschreibt die Hauptstrahlungsrichtung der Zelle den Winkel in Grad [°] zwischen geografisch-Nord und dem Hauptstrahl. Bei einer komplexen Zelle mit mehreren verschiedenen Hauptstrahlungsrichtungen und bei einer omnidirektionalen Zelle (gleichmässige Abstrahlung in alle Richtungen) ist dieses Datenfeld hingegen leer. Soweit verfügbar ist der Typ der benutzten Mobilfunktechnologie mitzuteilen. Bei 2G und 3G ist diese Mitteilung nicht möglich, da nicht im Standard vorhanden. Bei 4G ist es möglich. Dort gibt es den Parameter "Radio Access Technology (RAT)", der "4G" oder "WiFi" enthalten kann.

Buchstabe c stellt eine alternative Möglichkeit zu *Buchstabe a* und *b* dar. Die Bestimmung verweist lediglich auf die bisher geltenden und zukünftigen internationalen Standards, welche die Mitteilung der Standortangaben betreffen. Dadurch soll verhindert werden, dass die Verordnung jedes Mal angepasst werden muss, wenn die entsprechenden internationalen Standards angepasst beziehungsweise solche neu erlassen werden.

Art. 55 Überwachungstyp RT_23_NA_CC_IRI: Echtzeitüberwachung von Inhalten und Randdaten bei Netzzugangsdiensten

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ PS 1. Im Rahmen dieses Überwachungstyps hat die Mitwirkungspflichtige den gesamten Fernmeldeverkehr, der über den überwachten Netzzugang, beispielsweise mobiler Internetzugang gesendet (upload) oder empfangen (download) wird, das heisst, die Inhaltsdaten (Communication Content) sowie die zugehörigen Randdaten (IRI), die in Artikel 54 aufgeführt sind, in Echtzeit auszuleiten.

Wie bei Artikel 50 Absatz 4 erläutert, muss die Mitwirkungspflichtige grundsätzlich sicherstellen, dass jeglicher über die von ihr kontrollierte Infrastruktur geführter Fernmeldeverkehr überwacht werden kann. Ausgeleitet werden muss aber nur derjenige Fernmeldeverkehr, der an den überwachten Netzzugang gerichtet ist, beziehungsweise von diesem stammt. Bei der Benutzung fremder inländischer Infrastruktur, zum Beispiel nationales Roaming, Mobile Virtual Network Operator (MVNO), hat die Mitwirkungspflichtige sicherzustellen,

dass der gesamte zu überwachende Fernmeldeverkehr von ihr oder von Dritten ausgeleitet wird.

Bei der Benutzung ausländischer Infrastruktur (z. B. Roaming im Ausland) ist der Fernmeldeverkehr nur insoweit zu überwachen, wie er von der Mitwirkungspflichtigen kontrolliert werden kann. Kontrolliert die Mitwirkungspflichtige jedoch die ausländische Infrastruktur, muss sie die zu überwachenden Kommunikationsinhalte und Randdaten vollständig ausleiten.

Eine Besonderheit stellen die mit einem Mobiltelefoniedienst assoziierten MMS-Dienste dar, da die Inhaltsdaten von MMS nicht als Anwendung (s. 9. Abschnitt), sondern am Netzzugang im Rahmen des hier definierten Überwachungstyps mitüberwacht werden. Gemäss den ETSI-Standards werden Inhaltsdaten von eingehenden und ausgehenden MMS-Mitteilungen als Teil des Datenstroms bei der Zugangsüberwachung ausgeleitet, das heisst die MMS-Überwachung ist automatisch bei der Zugangsüberwachung eines mobilen Internetzugangs inklusive. Allerdings werden für MMS-Mitteilungen bei der Echtzeitüberwachung des Netzzugangs keine MMS-spezifischen Randdaten ausgeleitet. Diese sind jedoch im Rahmen des Überwachungstyps RT_24_TEL_IRI (Art. 56) oder RT_25_TEL_CC_IRI (Art. 57) verfügbar.

Je nach Art des Netzzugangs (fix oder mobile) beziehungsweise Technologie liegen diesem Überwachungstyp die folgenden ETSI-Standards zugrunde:

- mobiler Netzzugang (GPRS, UMTS, EPS (LTE), WLAN-Interworking): ETSI TS 101 671, TS 133 108, TS 102 232-1, TS 102 232-7,
- fixer Netzzugang: ETSI TS TS 102 232-1, TS 102 232-3,
- TS 102 232-7.

9. Abschnitt: Typen der Echtzeitüberwachung von Anwendungen

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

Die Bestimmung definiert den standardisierten Überwachungstyp Echtzeitüberwachung von Telefonie- und Multimediadiensten (entspricht dem bisherigen Überwachungstyp CS 2 und CS 3), weshalb auf die Erläuterungen beim Artikel 57 verwiesen werden kann. Im Gegensatz zum Artikel 57 sind im Rahmen eines Überwachungsauftrages gemäss Artikel 56 lediglich die Randdaten des Fernmeldeverkehrs in Echtzeit auszuleiten, zu denen auch die Standortangaben gehören. Die einzige Ausnahme bilden die Inhaltsdaten von SMS, welche aus technischen Gründen in den Randdaten in Echtzeit enthalten sein können und deshalb zusammen mit diesen ausgeleitet werden können.

Absatz 1 hält fest, welche Randdaten in Echtzeit zu übermitteln sind. Die in *Buchstabe b* bezeichneten Informationen über Registrierungsereignisse und die entsprechenden Antworten beziehen sich zum Beispiel auf die SIP-Anfragemethode "REGISTER" (s. RFC 3261). Entsprechend ist unter Subskriptionsereignis zum Beispiel die SIP-Anfragemethode "SUBSCRIBE" (s. RFC 6665) zu verstehen. Mit den in *Buchstabe e* aufgeführten "technischen Änderungen" sind Ereignisse gemeint, die die technischen Eigenschaften des überwachten Dienstes verändern

oder die dessen Mobility Management betreffen, so zum Beispiel Bearer Modification oder Location Update. Bei ortsunabhängigen Diensten sind die verfügbaren momentanen Standortangaben zu liefern (Bst. e Ziff. 9), die in Absatz 2 näher beschrieben sind. Für Ausführungen zu den Standortangaben, siehe die Erläuterungen zu Artikel 54 Absatz 3.

Für ausgehende Verbindungen und Verbindungsversuche, die mit Hilfe der freien Wahl der Dienstanbieterin (Carrier Selection) hergestellt werden, hat die Anbieterin des Telefoniedienstes ebenfalls die Randdaten zu liefern.

Art. 57 Überwachungstyp RT_25_TEL_CC_IRI: - Echtzeitüberwachung von Inhalten und Randdaten bei Telefonie- und Multimediadiensten

Der in diesem Artikel definierte Überwachungstyp basiert auf den bisherigen Typen CS1, CS2 und CS3. Die Überwachung der klassischen leitungsvermittelten Telefoniedienste wird jedoch auf paketvermittelte Telefoniedienste und Multimediadienste ausgeweitet. Zu den Telefonie- und Multimediadiensten gehören auch die mit diesen konvergierenden Dienste, so insbesondere SMS, Voice Mail und RCS (bezüglich der Begriffe und Abkürzungen, s. Anhang 1). Unter *konvergierenden Diensten* sind alle Anwendungen zu verstehen, welche die Mitwirkungspflichtige dem Teilnehmenden in engem Zusammenhang mit dem Telefonie- und Multimediadienst beziehungsweise als Teil von diesem erbringt, so beispielsweise Mobiltelefonie mit SMS, VoiceMail und RCS oder Festnetztelefonie konvergierend mit Mobiltelefonie. Sogenannte Multiple-Play-Produkte, bei denen verschiedene Dienste wie Telefonie, Internetzugang und TV in einem Paket vermarktet werden, gehören jedoch nicht zu den konvergierenden Diensten.

Ein bekanntes Beispiel für paketvermittelte Telefoniedienste ist Voice over IP (VoIP), auch Internet-Telefonie genannt. Im Bereich Mobiltelefonie sind in erster Linie VoLTE (Voice over LTE, d.h. Mobiltelefonie in 4G-Netzen) und VoWLAN (Mobiltelefonie über Wireless LAN, sog. non-3GPP Access) zu nennen. Im Bereich Multimediadienste gibt es beispielsweise ViLTE (Video over LTE, d.h. Videotelefonie in 4G-Netzen).

Die Telefonie- und Multimediadienste werden in der Regel als Anwendung überwacht und nicht am Netzzugang. Zwar sind bei Mobiltelefonie und leitungsgebundener Telefonie die Anbieterinnen des Zugangs (z. B. Telefonanschluss oder Mobilfunkzugang) und der Anwendung (Telefoniedienst) oft noch identisch, jedoch ist diese Kopplung bei modernen Diensten wie VoIP nicht mehr unbedingt gegeben. Auch in den klassischen Telefonnetzen schreitet die Entbündelung der Anschlüsse voran und es gibt die freie Wahl der Dienstanbieterin (Carrier Selection; Art. 9 der Verordnung der Eidgenössischen Kommunikationskommission vom 17. November 1997[50] betreffend das Fernmeldegesetz). Im Mobilfunkbereich sind bei einem Mobile Virtual Network Operator (MVNO) und beim Roaming die Anbieterin des Funkzugangsnetzes (Radio Access Network) und die Dienstanbieterin nicht identisch. Im IP Multimedia Subsystem (IMS) kann der Netzzugang auch über Netze anderer Anbieterinnen erfolgen, die keine Mobilfunknetze sind (sog. non-3GPP Access).

50 SR **784.101.112**

Dies sind nur einige Beispiele, bei denen die Netzzugangsanbieterin nicht identisch ist mit der Dienstanbieterin des Teilnehmenden.

Im Rahmen dieses Überwachungstyps hat die Mitwirkungspflichtige den gesamten Fernmeldeverkehr, der über den überwachten Telefonie- und Multimediadienst und die mit diesem konvergierenden Dienste abgewickelt wird, das heisst die Inhaltsdaten (Communication Content) sowie die zugehörigen Randdaten (IRI), die in Artikel 56 aufgeführt sind, in Echtzeit auszuleiten.

Für ausgehende Verbindungen und Verbindungsversuche, die mit Hilfe der freien Wahl der Dienstanbieterin (Carrier Selection) hergestellt werden, hat die Anbieterin des Telefoniedienstes ebenfalls die Inhalts- und Randdaten zu liefern.

Art. 58 Überwachungstyp RT_26_EMAIL_IRI: Echtzeitüberwachung von Randdaten bei E-Mail-Diensten

Die Bestimmung definiert analog zu Artikel 59 den standardisierten Überwachungstyp Echtzeitüberwachung von E-Mail-Diensten (entspricht dem bisherigen Überwachungstyp PS 4). Gemäss bisherigem Recht war eine E-Mail-Anbieterin jedoch nur dann verpflichtet, eine E-Mail-Überwachung auszuführen, wenn sie zugleich auch Internetzugangsanbieterin war (Art. 15 Abs. 4 BÜPF vom 6.10.2000)[51]. Neu entfällt diese Einschränkung. Die Überwachung und Ausleitung erfolgt technisch nur noch gemäss dem ETSI-Standard TS 102 232-2. Die frühere Schweizer proprietäre Lösung wird nur noch während einer Übergangszeit (s. Art. 74) unterstützt.

Im Gegensatz zum Artikel 59 sind im Rahmen eines Überwachungsauftrages gemäss Artikel 58 lediglich die Randdaten des überwachten E-Mail-Kontos in Echtzeit auszuleiten. Dazu gehören die SMTP-Envelop-Informationen. Im Rahmen dieses Überwachungstyps dürfen keine Inhaltsdaten ausgeleitet werden, also beispielsweise nicht der E-Mail-Header mit dem Betreff (subject).

Es sind sowohl die Mail-Server-Operationen, wie Mail Send, Mail Receive, Speichern der E-Mail im Message Store (Mailbox), als auch die Zugriffe von Mail Clients auf den Mail Server zu überwachen, das heisst Operationen wie das Anmelden und Abmelden des Benutzers an der Mailbox beziehungsweise entsprechende Versuche (*Bst. a*), das Herunterladen einer E-Mail von der Mailbox oder das Löschen einer E-Mail. Die wichtigsten Parameter der Randdaten sind in den Buchstaben a-d aufgeführt. Dazu gehören auch die AAA-Informationen ohne Passwort (*Bst. b*). Die Ereignisse, für die ein IRI zu generieren ist, sind in *Buchstabe d* summarisch dargestellt. Die Einzelheiten sind im ETSI-Standard TS 102 232-2 und im Anhang 1 der VD-ÜPF definiert. Zu beachten ist, dass auch interne E-Mails, das heisst Mailboxen, die vom gleichen Mail Server bedient werden, zu überwachen sind und dass auch die zum überwachten E-Mail-Konto zugehörigen Alias-Adressen und Verteilerlisten mit überwacht werden (zu den Begriffen Alias-Adresse und Mailingliste, s. die Erläuterungen zu Art. 42).

51 Siehe auch BBl **1998** 4279 ad Art. 13 Abs. 3.

Art. 59 Überwachungstyp RT_27_EMAIL_CC_IRI: Echtzeitüberwachung von Inhalten und Randdaten bei E-Mail-Diensten

Der in diesem Artikel definierte Überwachungstyp basiert auf dem bisherigen Typ PS3. Es sind sowohl die Inhalts- als auch die Randdaten des überwachten E-Mail-Kontos in Echtzeit auszuleiten (s. die Erläuterungen zu Art. 58). Die Anbieterin hat von ihr angebrachte Verschlüsselungen zu entfernen (Art. 26 Abs. 2 Bst. c BÜPF).

10. Abschnitt: Typen der rückwirkenden Überwachung

Die zum Zwecke der rückwirkenden Überwachung (Art. 26 Abs. 4 BÜPF) und der Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 BÜPF) gesammelten Randdaten werden in der Fachsprache als «aufbewahrte Daten» («retained data») bezeichnet. Umgangssprachlich werden auch die Begriffe Vorratsdaten und Vorratsdatenspeicherung verwendet, da die Randdaten aller Teilnehmenden sozusagen auf Vorrat gespeichert werden. Im BÜPF wird die Formulierung *aufbewahrte Randdaten des vergangenen Fernmeldeverkehrs* (Art. 26 Abs. 4 BÜPF) verwendet. Da die Überwachung des vergangenen Fernmeldeverkehrs als *rückwirkende Überwachung* bezeichnet wird, gibt es auch noch die alternative Formulierung *Randdaten des vergangenen Fernmeldeverkehrs*. Im 3. Kapitel, das ausschliesslich dem Fernmeldeverkehr gewidmet ist, wird in den Erläuterungen eher die Kurzform *aufbewahrte Randdaten* verwendet. Hinweis: Auch im Postverkehr gitb es die rückwirkende Überwachung (s. Art. 16 Bst. c).

Gestützt auf die Kompetenz, die dem Bundesrat in Artikel 31 BÜPF übertragen wird, werden im 10. Abschnitt des 3. Kapitels die Randdaten bestimmt, welche zum Zwecke der rückwirkenden Überwachung aufzubewahren und zu liefern sind.

Die zum Zwecke der Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 BÜPF) aufzubewahrenden Randdaten werden im Artikel 21 Absatz 2 bestimmt.

Die aufbewahrten Randdaten des vergangenen Fernmeldeverkehrs, das heisst die Randdaten, die bei einer rückwirkenden Überwachung beschafft werden, sind nicht identisch mit den Randdaten in Echtzeit (IRI), die bei einer Echtzeitüberwachung ausgeleitet werden. Beispielsweise liefert eine Echtzeitüberwachung auch Randdaten zu Ereignissen, die nicht im Zusammenhang mit Kommunikationen oder Kommunikationsversuchen stehen (z. B. Location Update). Andererseits gibt es auch Anwendungen (z. B. MMS), für die spezifische *aufbewahrte Randdaten* standardisiert sind, aber keine spezifischen Echtzeit-Randdaten (IRI).

Gemäss den Erläuterungen in der Botschaft zum BÜPF vom 27. Februar 2013 betreffend Artikel 26 Absatz 1 Buchstabe b BÜPF[52] müssen nunmehr nicht nur die Randdaten von erfolgreichen Kommunikationen, Anmeldungen (Login) beziehungsweise Herstellungen des Netzzugangs, sondern auch jene von Kommunikationsversuchen aufbewahrt werden.

Bei Telefonie- und Multimediadiensten gilt in diesem Sinne als Kommunikationsversuch, wenn die Verbindung erfolgreich aufgebaut wurde, der Kommunikationsaufbau aber unbeantwortet bleibt oder das Netzwerkmanagement

52 BBl **2013** 2739.

eingegriffen hat. Im Folgenden seien zwei Beispiele für Kommunikationsversuche genannt: 1. Der Anrufer wählt eine gültige Nummer, lässt es kurz klingeln und legt sofort wieder auf; 2. Der Anrufer wählt eine gültige Nummer und erhält die Ansage, dass der angerufene Teilnehmer momentan nicht erreichbar ist. Wenn der Anrufer im zweiten Beispiel dagegen auf eine VoiceMail weitergeleitet wird, stellt dies bereits eine Kommunikation dar. Ein Gegenbeispiel in diesem Sinne, welches weder eine Kommunikation, noch einen Kommunikationsversuch darstellt, ist die Wahl einer unvollständigen oder nicht-existenten Nummer.

Bei den E-Mail-Diensten und Mitteilungsdiensten gibt es in diesem Sinne keine Kommunikationsversuche, da bereits eine erfolgreiche Übermittlung der E-Mail beziehungsweise Mitteilung an den Mailserver beziehungsweise Messaging Server als Kommunikation gilt, selbst wenn die Übermittlung der E-Mail beziehungsweise Mitteilung an den Empfänger danach scheitern sollte. Dementsprechend gibt es auch bei den anderen Fernmelde- und abgeleiteten Kommunikationsdiensten keine Kommunikationsversuche.

Die Randdaten von Kommunikationsversuchen müssen jedoch nur nach Massgabe des Artikels 50 Absatz 4 von der Mitwirkungspflichtigen aufbewahrt werden. Wenn beispielsweise Anrufversuche von anderen Netzen abgebrochen werden, bevor die Signalisierung das Netz der Mitwirkungspflichtigen erreicht (in diesem Fall klingelt das angerufene Telefon nicht), kann die Mitwirkungspflichtige die Randdaten solcher Kommunikationsversuche nicht aufbewahren, da sie bei ihr technisch nicht vorhanden sind.

Weiterhin kann es vorkommen, dass Kommunikationen und Kommunikationsversuche nur unvollständige Adressierungselemente enthalten oder manche Adressierungselemente fehlen. Beispielsweise könnte bei Anrufen aus dem Ausland die Nummer des Anrufenden unvollständig sein oder sogar fehlen. Die entsprechend aufbewahrten Randdaten würden dann bei einer rückwirkenden Überwachung dieser ausländischen Nummer (Target ID) nicht gefunden werden können, da in diesem Beispiel die überwachte Nummer (Target ID) in den entsprechenden aufbewahrten Randdaten unvollständig beziehungsweise nicht vorhanden wäre.

Für alle Typen der rückwirkenden Überwachung (Art. 60-66) gilt, dass die dort beschriebenen *aufbewahrten Randdaten* auf dem ETSI-Standard TS 102 657 basieren.

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

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Überwachungstyp PS5 und dient zur rückwirkenden Überwachung eines Internetzugangs. Dabei werden die aufbewahrten Randdaten des vergangenen Fernmeldeverkehrs übermittelt, der über den überwachten Netzzugangsdienst gesendet oder empfangen wurde.

Die *Buchstaben a-i* halten fest, welche Daten die betreffenden Mitwirkungspflichtigen zu speichern und zu liefern haben. Es handelt sich um folgende Daten: das Datum und die Uhrzeit, wann der Netzzugang hergestellt und wann er getrennt wurde (*Bst. a*), alternativ kann statt des Endes die Dauer angegeben werden; der Typ (z. B. xDSL, Kabelmodem, WLAN, Mobilfunk) und der Status (z. B. erfolgreich) des Netzzugangs (*Bst. b*); der Identifikator, der für die

Authentifizierung des Benutzenden am überwachten Zugangspunkt verwendet wurde, zum Beispiel Benutzername (*Bst. c*); die dem Target durch die Netzzugangsanbieterin zugeteilten IP-Adressen beziehungsweise Adressbereiche und deren Typ (*Bst. d*). Sofern verfügbar sind ausserdem der eindeutige Geräteidentifikator des benutzten Endgeräts des Targets (*Bst. e*) und die jeweiligen Datenmengen, welche innerhalb der Sitzung hochgeladen und heruntergeladen wurden (*Bst. f*) zu speichern und zu liefern.

Die Standortangaben (*Bst. g und h*) entsprechen dem Standort der Zellenantenne, die das Mobilfunk-Target für den paketvermittelten Netzzugang bedient oder dem Standort des öffentlichen WLAN-Zugangspunktes, der das Target über WLAN bedient. Es müssen die Standortangaben am Anfang und am Ende jeder Netzzugangs-Sitzung des Targets geliefert werden, die im Überwachungszeitraum stattgefunden hat, d. h. der Anfang oder das Ende der Sitzung oder beide liegen im Überwachungszeitraum). Soweit verfügbar sind auch die Standortangaben während der Sitzung zu liefern.

Bei Netzzugang über Mobilfunk sind zusätzlich zu den in den Buchstaben a-f erwähnten Daten die Standortangaben zu übermitteln (*Bst. g*). Die Mitwirkungspflichtige hat bei der Übermittlung der Standortangaben gemäss Buchstabe g die Wahl zwischen drei verschiedenen Varianten.

Bei Netzzugang über öffentliches WLAN (*Bst. h*) sind zusätzlich zu den in den Buchstaben a-f erwähnten Daten die folgenden Informationen zu übermitteln:

- die BSSID (MAC-Adresse des Zugangspunktes);
- falls vorhanden die SSID (in menschenlesbarer Form);
- falls vorhanden die Standortangaben in Form von geografischen Koordinaten und / oder der Postadresse des vom Target benutzten WLAN-Zugangspunktes;
- der Benutzername, wie von der Mitwirkungspflichtigen zur Kenntnis genommen (Überprüfung nicht erforderlich);
- der Typ der Benutzerauthentifizierung (z. B. SMS, EAPSIM, Voucher);
- die vorhandenen zusätzlichen Informationen über die Benutzerauthentifizierung (Telefonnummer, MAC-Adresse, falls zutreffend die IMSI, für die Authentifizierung benutzter Benutzeridentifikator und Password); und
- die IP-Adresse des WLAN-Zugangspunktes;

Bei Netzzugang über Mobilfunk oder öffentliches WLAN sind ausserdem, falls zutreffend, die vorhandenen Standortinformationen aus der Seeschifffahrt (Schiffsname und Schiffsnummer) oder der Luftfahrt (Code der Fluggesellschaft, Registration des Luftfahrzeugs gemäss Luftfahrzeugregister, Flugnummer der Fluggesellschaft) zu übermitteln.

Bei Festnetz-Zugang (*Bst. i*) sind zusätzlich zu den in den Buchstaben a-f erwähnten Daten die Adressierungselemente des Netzzugangs und falls vorhanden dessen Postadresse zu übermitteln.

Art. 61 Überwachungstyp HD_29_TEL: rückwirkende Überwachung von Randdaten bei Telefonie- und Multimediadiensten

Der in diesem Artikel definierte Überwachungstyp basiert auf dem bisherigen Typ CS4 (rückwirkende Überwachung eines Telefoniedienstes) und wurde um die Multimediadienste erweitert. Er dient zur rückwirkenden Überwachung von Telefonie- und Multimediadiensten, das heisst zur Beschaffung der aufbewahrten Randdaten dieser Dienste. Die Begriffe *Telefonie- und Multimediadienste* und *konvergierende Dienste* werden bei Artikel 57 erläutert. Was unter einem *Kommunikationsversuch* zu verstehen ist, wurde einleitend zum 10. Abschnitt erläutert (s. oben).

Für ausgehende Verbindungen und Verbindungsversuche, die mit Hilfe der in den Erläuterungen zu Artikel 57 beschriebenen freien Wahl der Dienstanbieterin (Carrier Selection) hergestellt wurden, hat die Anbieterin des Telefoniedienstes ebenfalls die Randdaten zu liefern. Die Mitwirkungspflichtige muss in der Lage sein, bei der rückwirkenden Überwachung die Übereinstimmung von E.164-Nummern zu erkennen, auch wenn sie in verschiedenen Formaten (national, international) vorliegen.

Im Gegensatz zur Echtzeitüberwachung, bei der die MMS-Dienste am Netzzugang mitüberwacht werden, überwacht man sie rückwirkend als Anwendung, jedoch nicht als eigenständige Überwachung, sondern im Rahmen des hier definierten Überwachungstyps.

Im Standard sind zwei verschiedene Datenstrukturen für die Lieferung der historischen Daten von Telefonie- und Multimediadiensten vorgesehen. Auf die einzelnen Besonderheiten wird hier jedoch nicht eingegangen.

Die Standortangaben entsprechen dem Standort der Zellenantenne, die das Mobilfunk-Target bedient, dem Standort des öffentlichen WLAN-Zugangspunktes, der das Target über WLAN bedient oder dem Standort des Netzzugangs bei Multimediadiensten. Es müssen die Standortangaben am Anfang und am Ende jeder Kommunikation beziehungsweise -versuches des Targets geliefert werden, die im Überwachungszeitraum stattgefunden hat, d. h. der Anfang oder das Ende der Kommunikation beziehungsweise -versuches oder beide liegen im Überwachungszeitraum. Soweit verfügbar sind auch die Standortangaben während der Kommunikation zu liefern. Bei Multimediadiensten gilt die Sitzung als Kommunikation. Falls vorhanden sind zusätzliche Standortinformationen aus der Seeschifffahrt (Schiffsname und Schiffsnummer) oder der Luftfahrt (Code der Fluggesellschaft, Registration des Luftfahrzeugs gemäss Luftfahrzeugregister, Flugnummer der Fluggesellschaft) zu übermitteln.

Die *Buchstaben a-i* halten fest, welche Daten die betreffenden Mitwirkungspflichtigen zu speichern und zu liefern haben. Es handelt sich um folgende Daten:

a. die Art der Kommunikation (z. B. leitungsvermittelte Festnetztelefonie, leitungsvermittelte Mobiltelefonie, SMS, MMS, Multimedia Festnetz, Multimedia Mobile), das Datum und die Uhrzeit des Beginns der Kommunikation sowie gegebenenfalls (d.h. beispielsweise bei SMS und MMS nicht erforderlich) des Endes der Kommunikation oder alternativ deren Dauer. Bei Kommunikationsversuchen sind deren Art, Beginn-Datum und Beginn-Uhrzeit anzugeben;

b. die Adressierungselemente (z. B. MSISDN, E.164-Nummer, SIP URI, IMPU) aller Kommunikationsbeteiligten und deren Rollen (z. B. Anrufer, Angerufener, Auslöser der Weiterleitung, Ziel der Weiterleitung);

c. der Grund für das Ende der Kommunikation oder des Kommunikationsversuches (z. B. normal, besetzt, keine Antwort beziehungsweise bei SIP der entsprechende Code);

d. bei Mobilfunk (bei Multimediadiensten soweit verfügbar): die IMEI des benutzten Endgeräts des Targets und die IMSI des Targets;

e. falls zutreffend, der Typ des Trägerdienstes (Bearer Service, z. B. Sprache, Daten, Fax);

f. bei SMS und MMS: die Informationen über das Ereignis (SMS-Ereignis, MMS-Ereignis), den Typ der SMS und den Status (SMS-Status, MMS-Status);

g. bei Mobilfunk: die Standortangaben der vom Target benutzten Zelle zu Beginn und am Ende der Kommunikation oder des Kommunikationsversuches:
   1. die Zell- und Gebietsidentifikatoren, die geografischen Koordinaten und gegebenenfalls die Hauptstrahlungsrichtungen und die Postadresse, oder
   2. die vom Netzwerk berechneten Positionen des Targets (z. B. in Form von geografischen Koordinaten und dem zugehörigen Unsicherheitswert oder in Form von Polygonen unter Angabe der geografischen Koordinaten jedes Polygonpunktes) sowie die zugehörigen Postadressen, oder
   3. andere Angaben zu den Standorten des Targets oder der von diesem benutzten Zellen, gemäss internationalen Standards sowie die zugehörigen Postadressen;

h. bei Multimediadiensten:
   1. die IP-Adresse des Clients und deren Typ und die Portnummer,
   2. der Kommunikations-Korrelationsidentifikator,
   3. die Typen der Multimediainhalte,
   4. die Informationen über die Multimediakomponenten (Zeit, Name, Beschreibung, Initiator, Zugangs-Korrelationsidentifikator), und
   5. falls zutreffend, die Informationen über die IMS-Dienste (Typ des benutzten IMS-Dienstes, Rolle des Netzelements, von dem die Randdaten stammen); und

i. bei Multimediadiensten: die Informationen über den Netzzugang des Targets:
   1. der Zugangstyp (z.B. 3GPP E-UTRAN TDD),
   2. die Zugangsklasse (z.B. 3GPP HSPA),
   3. ob die Informationen über den Netzzugang vom Netzwerk stammen (Standortangaben, die nicht als vom Netzwerk stammend gekennzeichnet sind, also vom Endgerät oder von einer Applikation stammen könnten, sind weniger vertrauenswürdig, da sie verfälscht sein können), und

4. die Standortangaben über den Netzzugang zu Beginn und am Ende der Multimediasitzung sowie soweit verfügbar während der Multimediasitzung:
   - bei Netzzugang über Mobilfunk: die Standortangaben der vom Target benutzten Zelle gemäss Buchstabe g, oder
   - bei Netzzugang über WLAN: die verfügbaren Standortangaben des vom Target benutzten WLAN-Zugangspunktes (geografische Koordinaten, Postadresse), oder
   - bei Festnetz-Zugang: die verfügbare Postadresse des vom Target benutzten Zugangs.

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

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ PS6 (rückwirkende Überwachung eines asynchronen elektronischen Postdienstes). Die *Buchstaben a* und *b* halten fest, welche Daten die betreffenden Mitwirkungspflichtigen zu speichern und zu liefern haben. Der Schwerpunkt liegt dabei auf den Ereignissen Senden und Empfangen einer Nachricht sowie An- und Abmeldevorgängen an der Mailbox. Die Informationen zu den weiteren Ereignissen sind nur soweit vorhanden aufzubewahren und zu liefern. Mit dieser flexiblen Regelung wird berücksichtigt, dass viele Anbieterinnen von E-Mail-Diensten bereits seit langem ihre Anlagen in Betrieb haben, die die Überwachung der Schwerpunktereignisse unterstützen. Für die Überwachung der weiteren Ereignisse müssten diese Systeme jedoch angepasst werden, was nicht verhältnismässig wäre. Bei neuen Systemen sollen jedoch alle der in den Buchstaben a und b angegebenen Daten aufbewahrt und geliefert werden.

Art. 63 Überwachungstyp HD_31_PAGING: Bestimmung der letzten Aktivität des mobilen Endgerätes der überwachten Person

Der Überwachungstyp HD_31_PAGING umfasst die Bestimmung der letzten durch die Mobilfunkanbieterin festgestellten Aktivität (Netzzugangsdienste sowie Telefonie- und Multimediadienste) des mobilen Endgerätes der überwachten Person. Er entspricht technisch dem neuen Typ der Notsuche EP_35_PAGING, welcher auf dem bisherigen Typ der Notsuche N1 basiert. Damit steht diese bisher der Notsuche vorbehaltene Form der Überwachung neu auch als Überwachungsmassnahme in Strafverfahren nach Artikel 273 StPO beziehungsweise Art. 70d MStP zur Verfügung.

Art. 64 Überwachungstyp AS_32_PREP_COV: Netzabdeckungsanalyse in Vorbereitung eines Antennensuchlaufs

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ CS5 (Netzanalyse in Vorbereitung eines Antennensuchlaufes).

Um einen Antennensuchlauf vorzubereiten, kann die anordnende Behörde beim Dienst ÜPF eine Auflistung der Mobilfunkzellen oder WLAN-Zugangspunkte (WLAN access points) verlangen, die eine gewisse geografische Position zu einer bestimmten Zeit am wahrscheinlichsten abdeckten (*Abs. 1*). Die geografische Position ist entweder mittels Koordinaten oder mittels Postadresse

(s. Erläuterungen zu Art. 67 Bst. a Ziff. 1) zu bezeichnen. Weitere Angaben wie beispielsweise Tageszeit können zu einer genaueren Bestimmung der geografischen Position beitragen. Es ist jedoch nicht zwingend, weitere Angaben zu machen.

Absatz 2 definiert, welche Angaben die FDA dem Dienst ÜPF aufgrund der Anfrage liefern muss.

Art. 65 Überwachungstyp AS_33_PREP_REF: Referenzkommunikationen oder Referenznetzzugänge in Vorbereitung eines Antennensuchlaufs

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ CS7 (Netzanalyse mittels Referenzanrufen der Strafverfolgungsbehörden in Vorbereitung eines Antennensuchlaufes).

Wie Artikel 64 dient dieser Artikel dazu, einen Antennensuchlauf vorzubereiten. Die anordnende Behörde liefert dem Dienst ÜPF eine Liste von Referenzgesprächen, beziehungsweise von Referenzkommunikationen und Referenznetzzugängen zur weiteren Abklärung der betroffenen Mobilfunkzellen oder WLAN-Zugangspunkte (WLAN access points).

Absatz 2 legt die Angaben fest, welche die anordnende Behörde dem Dienst ÜPF für den Auftrag liefern muss. Die FDA benötigen diese Angaben, um die Mobilfunkzellen beziehungsweise die WLAN-Zugangspunkte bestimmen zu können.

Absatz 3 regelt, wie die FDA ihre Systeme aufgrund der in Absatz 2 genannten Suchkriterien durchsuchen müssen und definiert die Angaben, welche die FDA dem Dienst ÜPF liefern muss.

Art. 66 Überwachungstyp AS_34: Antennensuchlauf

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ CS6 (Antennensuchlauf) und beinhaltet neu ebenfalls die PS Kommunikation.

Dieser Artikel regelt, welche Angaben durch die FDA zu liefern sind.

Als Voraussetzung für den Überwachungstyp AS_34: Antennensuchlauf ist nicht zwingend der Überwachungstyp AS_32_PREP_COV oder Überwachungstyp AS_33_PREP_REF erforderlich.

Absatz 1 definiert den Umfang der Überwachung und limitiert die Überwachung auf einen Zeitraum von zwei Stunden pro Anordnung. Diese maximale Zeitspanne entspricht der bisherigen Praxis und wurde deshalb festgelegt, um den damit verbundenen Aufwand zu minimieren, die grossen Datenmengen zeitlich einzugrenzen und dem Verhältnismässigkeitsgrundsatz Rechnung zu tragen. Falls ein längerer Zeitraum für die Strafverfolgungsbehörden von Interesse ist, ist dieser längere Zeitraum in mehrere Anordnungen zu je zwei Stunden aufzuteilen. Die Gebühren werden dabei pro Anordnung für die Dauer von zwei Stunden und pro Zelle berechnet. Soll zum Beispiel für die Zellen A, B und C bei der FDA Y für einen Zeitraum von 5 Stunden ein Antennensuchlauf durchgeführt werden, so ordnet die anordnende Behörde den Antennensuchlauf mittels insgesamt 9 Anordnungen gegenüber dem Dienst ÜPF wie folgt an: Anordnung 1 und 2 für Zelle A für jeweils 2 Stunden und Anordnung 3 für Zelle A für 1 Stunde, analog

Anordnungen 4, 5 und 6 für Zelle B und Anordnungen 7, 8 und 9 für Zelle C. Daraus resultieren Gebühren von neunmal den Gebührenansatz für einen Antennensuchlauf gemäss GebV-ÜPF. Das Zwangsmassnahmengericht hat jede Anordnung zu genehmigen. Hierbei muss es wegen der grossen Anzahl von Betroffenen dieser Massnahme, der Beurteilung der Verhältnismässigkeit besondere Bedeutung schenken. Dabei kann auch die Prüfung des Vorgehens zur Ermittlung einer möglichst (in Anbetracht der technischen Vorbedingungen und des Ermittlungszieles) kleinen resultierenden Schnittmenge an Verdächtigen herangezogen werden.

Absatz 2 regelt, dass die Überwachungsdaten gemäss Absatz 1 in der für die Artikel 60 und 61 festgelegten Weise zu übermitteln sind, weshalb auf die dortigen Erläuterungen verwiesen werden kann.

11. Abschnitt: Notsuche und Fahndung

Das Gesetz ermöglicht neu die Überwachung des Postverkehrs ausserhalb von Strafverfahren im Rahmen einer Notsuche (Art. 35 Abs. 1 BÜPF) oder Fahndung (Art. 36 Abs. 1 BÜPF). Lediglich der Prozess der Anordnung und Genehmigung einer Überwachung des Postverkehrs im Rahmen einer Notsuche oder Fahndung unterscheidet sich von einer Überwachung des Postverkehrs innerhalb eines Strafverfahrens. Dafür sind aber keine eigenen Überwachungstypen oder spezielle Regelungen in der Verordnung erforderlich.

Für die Überwachung des Fernmeldeverkehrs ausserhalb von Strafverfahren im Rahmen einer Notsuche (Art. 35 BÜPF) oder Fahndung (Art. 36 BÜPF) werden spezielle Regelungen in der Verordnung getroffen. Bei den Überwachungstypen der Notsuche (Art. 67) wurden im Gegensatz zu den gewöhnlichen Überwachungstypen die Überwachung von Netzzugang und Anwendungen jeweils zusammengefasst. Dies liegt zum einen darin begründet, dass es bei Notsuchen sehr schnell gehen muss, da eine schwere Gefährdung der Gesundheit oder des Lebens der gesuchten Person besteht und der Ablauf der Anordnung durch die anordnenden Behörden an den Dienst ÜPF und die Beauftragung von diesem an die Mitwirkungspflichtigen möglichst einfach zu gestalten ist. Zum anderen sollen rasch alle verfügbaren Informationen über die Person eingeholt werden, die Ziel der Notsuche ist und deshalb muss die Mitwirkungspflichtige alle Fernmeldedienste, die sie im Zusammenhang mit den angeordneten zu überwachenden Identifikatoren (Target ID) erbringt, entsprechend dem angeordneten Typ der Notsuche überwachen.

An dieser Stelle ist es wichtig klarzustellen, dass gemäss Artikel 35 Absatz 3 BÜPF ebenfalls technische Geräte gemäss Artikel 269bis StPO (z. B. IMSI-Catcher) im Rahmen einer Notsuche eingesetzt werden können und dass es gemäss Artikel 36 Absatz 2 BÜPF ebenfalls möglich ist, technische Geräte gemäss Artikel 269bis StPO (z. B. IMSI-Catcher) oder besondere Informatikprogramme gemäss Artikel 269ter StPO (z. B. GovWare) im Rahmen einer Fahndung zu verwenden.

Art. 67 Überwachungstypen EP: Notsuche

Dieser Artikel ersetzt den Artikel 16*a* der VÜPF vom 31. Oktober 2001, der sich auf die Suche und Rettung vermisster Personen bezieht. Das BÜPF ermöglicht neu im Rahmen der Notsuche im Bereich des Fernmeldeverkehrs die Überwachung der Kommunikationsinhalte (Bst. b). Bisher waren das sogenannte Paging (Bst. a), die Echtzeitüberwachung der Randdaten (Bst. c) und die rückwirkende Überwachung (Bst. d) möglich. Diese Typen der Notsuche werden beibehalten.

Buchstabe a definiert den Überwachungstyp Paging, mit dem die letzte festgestellte Aktivität des mobilen Endgerätes durch die Mitwirkungspflichtige in Erfahrung gebracht wird. Hierbei handelt es sich um die Standortbestimmung von mobilen Endgeräten. Es ist der letzte verfügbare Standort zu liefern, unabhängig davon, welche Technologie und welcher Netzzugangstyp mit dem Gerät benutzt wurde. Die Zusammenstellung der Angaben wird in *Buchstabe a* beschrieben. Der *eindeutige Identifikator des Mobilfunknetzes* besteht aus der Mobilfunk-Landeskennzahl (Mobile Country Code, MCC) und der Mobilfunk-Netzkennzahl (Mobile Network Code, MNC). Die Ziffern 1-3 behandeln unterschiedliche Methoden der Standortbestimmung. Die Mitwirkungspflichtige muss die Standort-bestimmung anhand einer der drei Ziffern durchführen und die darin beschriebenen Informationen liefern. Die in *Ziffer 1* aufgeführte *Postadresse* kann auch eine ähnliche geografische Beschreibung (z. B. Strassen-Nummer und Km-Angabe, Postleitzahl Gemeinde) des Standorts der Zelle sein, da es nicht für alle Antennenstandorte echte Postadressen gibt. Das Datenfeld *Hauptstrahlungsrichtung* kann auch leer sein oder mehrere verschiedene Hauptstrahlungsrichtungswerte und Attribute enthalten. Bei einer omnidirektionellen Zelle (gleichmässige Abstrahlung in alle Richtungen) ist dieses Datenfeld leer. Bei einer komplexen oder speziellen Zelle kann dieses Datenfeld zusätzlich zu den Hauptstrahlungsrichtungswerten beispielsweise auch folgende Attribute enthalten: inh (inhouse = Zelle innerhalb eines Gebäudes); tun (tunnel = zur Zelle gehören Repeater für die Funkabdeckung eines oder mehrerer Tunnel).

Buchstabe b definiert die Echtzeitüberwachung mit Inhalt und Randdaten im Rahmen einer Notsuche. Die anordnende Behörde erteilt eine Anordnung pro Mitwirkungspflichtige und pro gesuchtes Endgerät an den Dienst ÜPF, welcher dann die Notsuchen an die entsprechenden Mitwirkungspflichtigen beauftragt. Jede beauftragte Mitwirkungspflichtige richtet die jeweils zutreffenden Überwachungstypen gemäss den Artikeln 55 und 57 ein, so dass alle von ihr erbrachten Dienste für das gesuchte Endgerät abgedeckt sind. Damit wird der Dringlichkeit einer Notsuche Rechnung getragen, da es um die schnellstmögliche Standortbestimmung und Auffindung von Personen geht, die an Leib und Leben bedroht sind. Einzelne Aufträge pro überwachten Fernmeldedienst beziehungsweise abgeleiteten Kommunikationsdienst, wie sie sonst bei Überwachungen erteilt werden, würden bei einer Notsuche zu viel Zeit kosten. Beispiel: Die Mitwirkungspflichtige 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 Mitwirkungspflichtigen ein Mobilabonnement mit Telefonie und Internetzugang, dann richtet die Mitwirkungspflichtige entsprechend für den Telefoniedienst eine Echtzeitüberwachung von Inhalten und Randdaten bei Telefonie- und Multimediadiensten (Art. 57) und für den Netzzugang eine Echtzeitüberwachung von Inhalten und Randdaten bei Netzzugangsdiensten (Art. 55) ein. Die Echtzeitüberwachungen bleiben auch im Rahmen einer Notsuche so

lange aktiv, bis der Dienst ÜPF die jeweiligen Aufhebungsaufträge an die entsprechenden Mitwirkungspflichtigen erteilt.

Buchstabe c definiert die Echtzeitüberwachung ohne Inhaltsdaten, das heisst nur der Randdaten, im Rahmen einer Notsuche. Das Vorgehen ist entsprechend wie unter Buchstabe b erläutert. Der einzige Unterschied zu Buchstabe b besteht darin, dass jede beauftragte Mitwirkungspflichtige die jeweils zutreffenden Überwachungstypen gemäss den Artikeln 54 und 56 einrichtet, so dass alle von ihr erbrachten Dienste für das gesuchte Endgerät abgedeckt sind.

Buchstabe d regelt die rückwirkende Notsuche beispielsweise für den Fall, dass das Endgerät nicht mehr aktiv ist. Das Vorgehen ist entsprechend wie unter Buchstabe b erläutert. Die Unterschiede zu Buchstabe b bestehen darin, dass es sich um rückwirkende Überwachungen handelt, dass jede beauftragte Mitwirkungspflichtige die jeweils zutreffenden Überwachungstypen gemäss den Artikeln 60 und 61 einrichtet, so dass alle von ihr erbrachten Dienste für das gesuchte Endgerät abgedeckt sind, und dass für die rückwirkenden Überwachungen keine Aufhebungsaufträge erforderlich sind.

Die Entschädigung für die Mitwirkungspflichtigen richtet sich nach der Anzahl der durch die Behörden angeordneten Notsuchen pro Mitwirkungspflichtige und pro gesuchtes Endgerät und nicht nach der Anzahl der letztlich durchgeführten Überwachungen.

Art. 68 Fahndung

Dieser Artikel ist neu und regelt die Fahndung nach verurteilten Personen wie in Artikel 36 BÜPF vorgesehen. Der Typ der Fahndungsanordnung besteht aus einem Überwachungstyp der Echtzeitüberwachung "Inhalt und Randdaten" (*Bst. a*) oder aus einem Überwachungstyp der Echtzeitüberwachung "nur Randdaten" (*Bst. b*) oder aus einem Überwachungstyp der rückwirkenden Überwachung (*Bst. c*). Die Fahndungstypen entsprechen exakt den Überwachungstypen. Bei den Fahndungstypen werden also im Unterschied zu den Typen der Notsuche keine Überwachungstypen kombiniert. Zur Unterscheidung in der Statistik muss bei der Anordnung solcher Fahndungen als Grund der Überwachung das Attribut "Fahndung" angegeben werden. Falls im Rahmen einer Fahndung mehrere Überwachungstypen angeordnet werden sollen, muss pro Überwachungstyp eine Anordnung erfolgen. Bei Fahndungen gilt die übliche Gebührenregelung, dass jeder der pro Anbieterin und zu überwachendem Identifikator (Target ID) angeordneten Überwachungstypen gebührenpflichtig ist (s. GebV-ÜPF).

12. Abschnitt: Netzexterne Identifikatoren

Art. 69

Dieser Artikel regelt, ähnlich wie die Artikel 16*b* und 24*c* der VÜPF vom 31. Oktober 2001, die Überwachung von netzexternen Identifikatoren. Netzexterne Identifikatoren sind Identifikatoren, die nicht von der mit der Überwachung beauftragten Mitwirkungspflichtigen verwaltet werden oder die nicht in ihrem Netz eingebucht sind.

Hiermit wird die sogenannte "Kopfschaltung" geregelt. Zur Vereinfachung werden in den folgenden Erläuterungen die Bezeichnungen "eigen" und "fremd" verwendet. Diese verstehen sich aus Sicht der mit der Überwachung beauftragten Anbieterin. Bei der "Kopfschaltung" geht es um die Überwachung "fremder" Identifikatoren, welche als Kommunikationspartner bei "eigenen" Diensten auftauchen. Es sind nur die Adressierungselemente auszuwerten. Es muss also insbesondere keine Inspektion von Inhaltsdaten durchgeführt werden. Sobald aus Sicht der mit der Überwachung beauftragten Anbieterin ein "eigener" Kunde über die "eigene" Anwendung (Telefonie- und Multimediadienst, E-Mail-Dienst) mit dem überwachten "fremden" Adressierungselement kommuniziert, ist diese Kommunikation zu überwachen, das heisst gemäss Überwachungstyp sind die entsprechenden Randdaten und gegebenenfalls Inhaltsdaten auszuleiten. Gängige Praxis ist schon seit Jahren die Telefonie-Kopfschaltung, bei der eine "fremde" Telefonnummer überwacht wird.

Die "Kopfschaltung" ist nur bei Anwendungen (Telefonie- und Multimediadienste, E-Mail-Dienste) standardisiert, jedoch nicht beim Netzzugang. Ausserdem bestehen bei den überwachten Identifikatoren (Target ID) gewisse Einschränkungen (z. B. ist bei Mobilfunkdiensten keine IMSI und keine IMEI möglich). Aufgrund der unterschiedlichen technischen Gegebenheiten je nach Anbieterin und zu überwachendem Fernmeldedienst wird empfohlen, dass die anordnende Behörde vor Anordnung der Überwachung die Beratung des Dienstes ÜPF in Anspruch nimmt, um die Machbarkeit abzuklären.

Im Unterschied zur bisherigen Praxis ist kein gesonderter Vermerk in der Überwachungsanordnung beziehungsweise im Überwachungsauftrag erforderlich.

Neu ist auch die Standardisierung einer "Kopfschaltung" bei E-Mail-Diensten: die Überwachung einer "fremden" E-Mail-Adresse bei einer E-Mail-Anbieterin, das heisst die Überwachung von eingehenden E-Mails an "eigene" E-Mail-Kunden von der "fremden" überwachten E-Mail-Adresse sowie umgekehrt die ausgehenden von "eigenen" E-Mail-Kunden an die "fremde" überwachte E-Mail-Adresse. Dabei sind wie eingangs erwähnt nur die Adressierungselemente im SMTP-Envelop auszuwerten. Aus technischen Gründen können bei einer E-Mail-"Kopfschaltung" nur Mail-Server-Operationen wie die Sende- und Empfangsvorgänge von E-Mails, nicht aber die Zugriffe auf die "fremde" Mailbox überwacht werden.

Zur Klarstellung sei angemerkt, dass es sich bei der "Kopfschaltung" nicht um eine Art der Kabelaufklärung handelt. Bezüglich des Begriffs "Kopfschaltung" wird ebenfalls auf die Erläuterungen in der Botschaft zum BÜPF vom 27. Februar 2013[53] betreffend Artikel 31 BÜPF verwiesen.

4. Kapitel: Schlussbestimmungen

Art. 70 Organisatorische, administrative und technische Vorschriften

Dieser Artikel entspricht Artikel 33 VÜPF vom 31. Oktober 2001[54] mit den nötigen Änderungen.

53 BBl **2013** 2749.
54 SR **780.11**

Artikel 70 ist, zusammen mit Artikel 31 Absatz 3 BÜPF[55], die rechtliche Grundlage für die Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF). Die Verordnung des EJPD über das Beratende Organ im Bereich der Überwachung des Post- und Fernmeldeverkehrs (Beratendes Organ) stützt sich dagegen direkt auf das BÜPF (Art. 5 Abs. 3 BÜPF).

Gestützt auf Artikel 70 erlässt das EJPD die für die Durchführung der Überwachung des Post- und Fernmeldeverkehrs erforderlichen technischen, administrativen und organisatorischen Bestimmungen. Diese richten sich nicht nur an die Anbieterinnen von Fernmeldediensten und abgeleiteten Kommunikationsdiensten, sondern auch an die Anbieterinnen von Postdiensten.

Nach bisherigem Recht wurden die technischen und administrativen Einzelheiten durch Richtlinien des Dienstes ÜPF geregelt (Art. 33 Abs. 1bis VÜPF vom 31. Oktober 2001[56]; s. www.li.admin.ch).

Weitere Delegationsnormen an das EJPD befinden sich in den Artikeln 33 (Abnahmeverfahren) und 49 Absatz 2 (technische Angaben in der Überwachungsanordnung) sowie im Artikel 29 Absatz 1 (Anforderungen an die Qualität der übermittelten Daten).

Der *zweite Satz* des Artikels 70 präzisiert, dass das EJPD die Fristen festsetzt, innerhalb derer die entsprechenden Daten zu liefern sind.

Art. 71 Vollzug

Absatz 1 entspricht im Wesentlichen dem Artikel 33 Absatz 2 VÜPF vom 31. Oktober 2001[57]. Mit dieser Regelung wird sichergestellt, dass der Dienst ÜPF weiterhin die elektronischen Formulare und Schnittstellen für alle anordnenden Behörden und Mitwirkungspflichtigen zur Verfügung stellen kann. Aus Gründen der Effizienz und Fehlervermeidung sind ausschliesslich die elektronischen Formulare und Schnittstellen des Dienstes ÜPF zu verwenden.

Absatz 2 sieht vor, dass zu einem späteren Zeitpunkt die elektronischen Formulare durch einen Online-Zugriff auf das Verarbeitungssystem des Dienstes ÜPF ersetzt werden können. Da dieser Zeitpunkt noch unbestimmt ist, kann der Dienst ÜPF selber über diese Umstellung entscheiden. Sollte der Online Zugriff auf das Verarbeitungssystem nicht möglich sein oder dieses selbst einmal ausfallen, so sollen die Formulare weiterhin zum Einsatz kommen.

Art. 72 Aufhebung eines anderen Erlasses

Mit dem Inkrafttreten der vorliegenden Verordnung wird die VÜPF vom 31. Oktober 2001 aufgehoben.

Art. 73 Änderung anderer Erlasse

Zwei andere Verordnungen werden gleichzeitig teilgeändert:

55 BBl **2013** 2750/2751.
56 SR **780.11**
57 SR **780.11**

- die Organisationsverordnung vom 17. November 1999[58] für das Eidgenössische Justiz- und Polizeidepartement (OV-EJPD). Es handelt sich hier um Anpassungen im Artikel 25.

- die Verordnung vom 9. März 2007[59] über Fernmeldedienste (FDV). Es geht um eine formelle Anpassung im Artikel 80.

Art. 74 Übergangsbestimmungen

Das BÜPF enthält Übergangsbestimmungen in Artikel 45. Teilweise ist es notwendig, diese zu präzisieren und weitere Übergangsbestimmungen vorzusehen. Somit kann auf ein gestaffeltes Inkrafttreten der Ausführungsverordnungen zum totalrevidierten BÜPF verzichtet werden.

Die Übergangsbestimmungen in Artikel 74 sind chronologisch angeordnet. Der massgebende Zeitpunkt des ersten bis sechsten Absatzes ist das Inkrafttreten dieser Verordnung, derjenige des siebten und achten Absatzes die Inbetriebnahme des neuen Verarbeitungssystems, das heisst der neuen Systemkomponenten, die mit dem Programm FMÜ beschafft werden.

Nach Artikel 45 Absatz 1 BÜPF sind auf bereits laufende Überwachungen allerdings insbesondere das neue Akteneinsichts- und Auskunftsrecht (Art. 10 BÜPF), das neue Aufsichtsrecht (Art. 41 BÜPF), der Rechtsschutz (Art. 42 BÜPF) und die Regelungen betreffend die Qualität der übermittelten Daten (Art. 18 BÜPF und Art. 29) anwendbar.

Teil des Übergangsprozesses ist, dass die anordnenden beziehungsweise berechtigten Behörden die bisherigen Auskunfts- und Überwachungstypen noch solange anordnen können, wie deren Beauftragung vom Dienst ÜPF an die Mitwirkungspflichtigen vor dem Zeitpunkt des Inkrafttretens dieser Verordnung erfolgen kann. Ab Inkrafttreten dieser Verordnung werden für neue Überwachungsanordnungen und Auskunftsgesuche der Behörden nur noch die neuen Auskunfts- und Überwachungstypen verwendet.

Da zum Zeitpunkt des Inkrafttretens dieser Verordnung noch zahlreiche Echtzeitüberwachungen aktiv sein werden, die vor Inkrafttreten dieser Verordnung, also gemäss bisherigem Recht angeordnet wurden, wird für diese eine Übergangsbestimmung in *Absatz 1* geschaffen. Nach Artikel 45 Absatz 1 BÜPF werden Überwachungen, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Gange sind, nach neuem Recht fortgeführt. Allerdings soll dabei die Durchführung der laufenden Untersuchungen nicht allzu stark kompliziert werden[60]. Deshalb ist davon auszugehen, dass der Gesetzgeber die Durchführung der laufenden Überwachungen nicht mit den neuen Überwachungstypen anwenden wollte, was dieses Ziel verunmöglichen würde. Absatz 1 sieht vor, dass solche Überwachungen unverändert weiterlaufen. Das Gegenteil wäre eine Aufhebung und Neuschaltung dieser Überwachungen, welche aus den folgenden Gründen die Durchführung der laufenden Untersuchungen stark komplizieren würde: Dies würde bei den

58 SR **172.213.1**
59 SR **784.101.1**
60 vgl. BBl **2013** S. 2768 zu Art. 45 Abs. 1 BÜPF

Behörden, dem Dienst ÜPF und den Mitwirkungspflichtigen einen unverhältnismässig hohen administrativen und technischen Aufwand und erhebliche Kosten verursachen. Aufgrund des Wechsels auf die neuen Überwachungstypen müssten diese laufenden Überwachungen neu von den Behörden angeordnet und entsprechend von den Zwangsmassnahmengerichten genehmigt werden. Dann müssten der Dienst ÜPF und die Mitwirkungspflichtigen diese Überwachungsmassnahmen neu schalten und die bisherigen aufheben. Ausserdem würden die laufenden Überwachungen jeweils in zwei Teile geteilt (alt, neu), was das Risiko von Datenverlusten erhöhen würde.

Für rückwirkende Überwachungen und Auskünfte gemäss bisherigem Recht, die zum Zeitpunkt des Inkrafttretens dieser Verordnung noch in Bearbeitung sind, gilt die obige Regelung sinngemäss. Sie werden gemäss bisherigem Recht ausgeführt und beantwortet.

Die Verlängerungen und Aufhebung der vorgenannten bestehenden Überwachungen erfolgen ebenfalls noch mit den bisherigen Überwachungstypen. Mit dem Begriff Verlängerungen sind die periodischen Verlängerungen von Echtzeitüberwachungen gemäss Artikel 274 StPO beziehungsweise Artikel 70e MStP gemeint. Dieser adminstrative Prozess wird nach wie vor zwischen der anordnenden Behörde, der Genehmigungsbehörde und dem Dienst ÜPF abgewickelt. Es kommen also auch hier während der Übergangszeit noch die bisherigen Überwachungstypen zur Anwendung. Damit wird auch dieser Prozess vereinfacht, da eine bereits vor Inkraftreten dieser Verordnung nach bisherigem Recht angeordnete Überwachung unverändert verlängert werden kann. Die Mitwirkungspflichtige, bei der die Echtzeitüberwachung aktiv ist, wird über eine Verlängerung wie auch bisher nicht informiert.

Aus technischen Gründen ist die Anwendung der bisherigen Überwachungstypen für die Aufhebung (Deaktivierung) von Überwachungen jedoch nur solange möglich, wie die bisherige Systemkomponente zur Auftragsverwaltung (AMIS) des Dienstes ÜPF noch in Betrieb ist. Im Rahmen des Programms FMÜ soll sie durch eine neue Systemkomponente ersetzt werden. Die neue Systemkomponente wird nur noch die neuen Überwachungstypen unterstützen. Ausgehend von der durchschnittlichen Dauer einer Echtzeitüberwachung wird bis zur Ablösung des AMIS durch die neue Systemkomponente der Grossteil der noch nach bisherigem Recht angeordneten Überwachungen ohnehin bereits regulär beendet worden sein. *Absatz 2* sieht vor, dass mit Inkrafttreten dieser Verordnung die nach bisheriger Praxis bestehenden Testschaltungen (s. Erläuterungen zu Art. 30) durch den Dienst ÜPF aufgehoben werden, da sie den bisherigen Überwachungstypen entsprechen, die kaum noch getestet werden müssen.

Absatz 3 sieht eine Übergangsbestimmung für die FDA vor, die ein Gesuch um Einstufung als FDA mit reduzierten Überwachungspflichten gemäss Artikel 51 einreichen möchten. Wenn die Gutheissung des Gesuchs wahrscheinlich ist, gelten sie bereits ab dem Moment der Einreichung des Gesuches als FDA mit reduzierten Überwachungspflichten und bleiben es bis zum Entscheid des Dienstes ÜPF. Diese Bestimmung wurde geschaffen, um diese FDA vor unnötigen Investitionskosten für die Anpassung ihrer Systeme zu bewahren, um die Überwachungsbereitschaft im

Zeitraum zwischen Inkrafttreten dieser Verordnung und dem Entscheid des Dienstes ÜPF sicherzustellen. Die FDA haben ab Inkrafttreten dieser Verordnung drei Monate Zeit, um beim Dienst ÜPF ein solches Gesuch einzureichen. Der Dienst ÜPF prüft die Angaben im Gesuch sowie die eingereichten Belege und entscheidet dann mittels Verfügung oder Zwischenverfügung im Sinne von Artikel 5, 45 und 46 des Bundesgesetzes vom 20. Dezember 1968 über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz; VwVG[61]), ob die Gesuchstellerin als FDA mit reduzierten Überwachungspflichten oder als FDA mit vollen Pflichten eingestuft wird. Der letzte Satz von Absatz 3 schliesst die Anwendung der Übergangsfrist in Artikel 51 Absatz 5 für FDA, welche nicht mehr als solche mit reduzierten Überwachungspflichten gelten, für eine bestimmte Gruppe von FDA aus. Nach bisherigem Recht meldepflichtige FDA, das heisst FDA, die auch Überwachungspflichten nach dem bisherigen BÜPF erfüllen mussten, könnten versucht sein, ein Gesuch einzig deshalb zu stellen, damit sie von den Übergangsfristen des Artikel 51 Absatz 5 profitieren können. Um dies zu vermeiden, schliesst der letzte Satz von Absatz 3 die Anwendung von Artikel 51 Absatz 5 für bisher meldepflichtige FDA aus. Der Dienst ÜPF stuft die FDA als FDA mit vollen Pflichten ein und bestimmt einzeln die Frist für die Speicherung der für die Überwachung erforderlichen Daten und diejenige für die Überwachungsbereitschaft.

Mit der Regelung in *Absatz 4* wurde der Forderung der Anbieterinnen nach einer Übergangsfrist entsprochen, um insbesondere die Verkaufsstellen von Mobilfunkdiensten für die Erfassung der Ausweiskopien technisch auszurüsten, die Systeme zur Erfassung der Teilnehmerdaten anzupassen und die Identifikation der Teilnehmenden beziehungsweise bei professionell betriebenen öffentlichen WLAN-Zugangspunkten der Endbenutzenden mit geeigneten Mitteln sicherzustellen.

Absatz 5 sieht vor, dass die Anbieterinnen, welche die Pflicht zur Aufbewahrung von Randdaten haben (s. Art. 21 Abs. 2 Bst. b) eine Frist von höchstens 6 Monaten nach Inkrafttreten dieser Verordnung haben, um ihre Systeme entsprechend anzupassen, damit sie die Auskünfte gemäss den Artikeln 38 (Identifikation der Benutzerschaft bei nicht eindeutig zugeteilten IP-Adressen [NAT]) und 39 (Auskünfte über NAT-Übersetzungsvorgänge) erteilen können (s. auch die Erläuterungen zu Art. 18 Abs. 4).

Absatz 6 sieht ab Inkrafttreten dieser Verordnung eine Übergangsfrist von 24 Monaten vor, bis die FDA bei der rückwirkenden Überwachung in der Lage sein müssen, die Randdaten zu Kommunikationsversuchen liefern zu können (*Bst. a*). Diese Frist ermöglicht es den FDA, ihre Systeme entsprechend anzupassen. Die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten gemäss Artikel 52 werden hier nicht erwähnt, da bei ihnen solche Systeme noch nicht vorhanden sind. Für sie gilt die Frist von 12 Monaten ab Entscheid des Dienstes ÜPF gemäss Artikel 52 Absatz 2 in Verbindung mit Artikel 22 Absatz 5. Die gleiche Übergangsfrist von 24 Monaten wird den FDA

61 SR **172.021**

eingeräumt, um ihre vorhandenen Systeme zur E-Mail-Überwachung gemäss den Vorschriften dieser Verordnung und der VD-ÜPF umzustellen (*Bst. b*). Die veralteten proprietären Schweizer Vorschriften für die E-Mail-Überwachung werden in der VD-ÜPF nämlich nicht mehr unterstützt. Das Verarbeitungssystem des Dienstes ÜPF unterstützt diese noch für bereits vor Inkrafttreten dieser Verordnung operationelle Systeme während dieser Übergangszeit.

Absatz 7 Buchstabe a gibt dem Dienst ÜPF die Möglichkeit, die Statistik noch nach bisherigem Recht vorzunehmen, bis die Systemkomponenten nach der Etappe 1 des Programms zum Ausbau und zum Betrieb des Verarbeitungssystems zur Fernmeldeüberwachung (V-FMÜ) sowie der polizeilichen Informationssysteme des Bundes (Programm FMÜ)[62] in Betrieb genommen werden. Die bisherigen Systeme, vor allem das CCIS, bei welchem der Wartungsvertrag nicht mehr angepasst werden kann, ermöglichen die nach neuem Recht verlangten Statistikauszüge nicht.

Weiter sieht *Buchstabe b* vor, dass bis zur Inbetriebnahme des neuen Verarbeitungssystems des Programms FMÜ, die neuen Auskunfts- (Art. 27 und 35-48) und Überwachungstypen (Art. 54-68) noch mit dem bestehenden System, den bisherigen Formaten und den entsprechenden Formularen abgewickelt werden. Die Auskunftsgesuche, die Aufträge an die Mitwirkungspflichtigen und deren Antworten werden mit einem durch den Dienst ÜPF zugelassenen sicheren Übertragungsmittel (s. Erläuterungen zu Art. 3 Abs. 1 Bst. a), per Post oder Telefax übermittelt. Für die nach dem Inkrafttreten dieser Verordnung gestellten Auskunftsgesuche und angeordneten Überwachungen gelten die neuen Auskunfts- und Überwachungstypen dieser Verordnung. Überwachungen, die vor dem Inkrafttreten dieser Verordnung angeordnet wurden, werden noch mit den bisherigen Überwachungstypen und den bisherigen Formaten im bestehenden System belassen. Das neue Recht ist allerdings auch auf diese Überwachungen anwendbar (Art. 45 Abs. 1 BÜPF), beispielsweise für die Aufsicht des Dienstes ÜPF (Art. 41 ff. BÜPF) und die Qualität der übermittelten Daten (Art. 28 VÜPF).

Buchstabe c ist in Verbindung mit Absatz 8 zu lesen. Weil das neue Verarbeitungssystem zum Zeitpunkt des Inkrafttretens dieser Verordnung noch nicht in Betrieb ist, können Auskunftsgesuche mit flexibler Namenssuche gemäss Artikel 27 vorerst noch nicht gestellt werden. Die FDA und die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten haben 12 Monate Zeit ab Inbetriebnahme des neuen Verarbeitungssystems, um ihre Systeme für die flexible Namenssuche anzupassen (Abs. 8). Falls eine gemäss Artikel 15 BÜPF berechtigte Behörde ab Inbetriebnahme des neuen Verarbeitungssystems ein Auskunftsgesuch mit flexibler Namenssuche stellt, kann dieses logischerweise nur von den Anbieterinnen beantwortet werden, die ihre Systeme bereits angepasst haben.

Absatz 8 definiert die Frist von 12 Monaten nach Inbetriebnahme des neuen Verarbeitungssystems, in welcher die FDA und die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten (Art. 22) ihre

62 BBl **2015** 3033

Systeme so anzupassen haben, dass sie in der Lage sind, die Auskünfte gemäss den Artikeln 34-36 und 39-41 automatisiert über die Abfrageschnittstelle des neuen Verarbeitungssystems zu erteilen. Die gleiche Frist gilt für die Anpassung ihrer Systeme, damit die Auskünfte mit flexibler Namenssuche durchgeführt werden können (s. Abs. 7 Bst. c). Die FDA mit reduzierten Überwachungspflichten (Art. 51) müssen gemäss Artikel 18 Absatz 3 keine automatisierte Auskunftserteilung über die Abfrageschnittstelle des neuen Verarbeitungssystems durchführen. Sie können sie jedoch freiwillig implementieren.

Art. 75 Inkrafttreten

Das Inkrafttreten dieser Verordnung wurde mit dem Inkrafttreten des BÜPF und der anderen Ausführungsverordnungen koordiniert.

Auf ein gestaffeltes Inkrafttreten kann verzichtet werden.

Anhang

Tabelle Pflichten PDA/FDA

		AUSKUNFT			ÜBERWACHUNG		
		BÜPF	VÜPF	Pflichten	BÜPF	VÜPF	Pflichten
Anbieterinnen von Postdiensten (**PDA**)		____	____	____	19	14	
Anbieterinnen von Fernmeldediensten (**FDA**) Art. 2 Bst. b BÜPF	KLEIN[63] (oder im Bildungs-bereich[64]) Art. 26 Abs. 6 BÜPF	21/22	11 Abs. 2 18 Abs. 1 und 3 21 31 (compliance)	A	26 Abs. 2 und 6	11 Abs. 2 51	B
	NORMAL	21/22	11 Abs. 2, 18 Abs. 1 und 2, 19, 20 21 31 (compliance) 74 (Übergangsbest.)	C	26 Abs. 1-5	11 Abs. 2 50 31 (compliance)	D
Anbieterinnen abgeleiteter Kommunikationsdienste Art. 2 Bst. c BÜPF	NORMAL	22 Abs. 3	11 Abs. 2 18 Abs. 4	E	27 Abs. 1 und 2	11 Abs. 2	F
	GROSS[65] (weitergehende Pflichten) Art. 27 BÜPF	22 Abs. 4	11 Abs. 2 18 Abs. 1 und 2 22 31 (compliance) 74 (Übergangsbest.)	G	27 Abs. 3 26 Abs. 1-5	11 Abs. 2 31 (compliance) 50 52	H

[63] Downgrade
[64] In den Verordnungen wird aufgrund eines Antrages in der Vernehmlassung der Begriff «Bildungsbreich» durch den Ausdruck «Bereich Bildung und Forschung» ersetzt
[65] Upgrade

A. Pflichten der FDA mit reduzierten Überwachungspflichten (Art. 51 VÜPF) bei Auskünften

Voraussetzung: FDA bietet Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bereich Bildung und Forschung an (Kriterien gemäss Art. 51 Abs. 1 und 2 VÜPF).

- haben bei Auskünften im Prinzip die gleichen Pflichten wie "normale" FDA (kein Downgrade bei Auskünften), d. h. müssen die Auskunftsbereitschaft sicherstellen (Art. 31 und 32 VÜPF)
- haben aber die folgenden Ausnahmen:
  - sie können die Auskünfte auch ausserhalb des Verarbeitungssystems schriftlich erteilen (Art. 18 Abs. 3 VÜPF), d. h.:
    - sie müssen sich nicht an die Abfrageschnittstelle des Verarbeitungssystems des Dienstes ÜPF anschliessen und
    - sie müssen die Auskünfte gemäss den Artikeln 35-37 und 40-42 VÜPF sowie gemäss Artikel 27 in Verbindung mit den Artikeln 35, 40 und 42 VÜPF nicht automatisiert erteilen
  - sie müssen die Auskünfte gemäss den Artikeln 38 und 39 VÜPF nicht im standardisierten Verfahren erteilen, sondern lediglich auf der Basis der ihnen zur Verfügung stehenden Randdaten
  - sind vom Pikettdienst befreit gemäss Artikel 11 Absatz 2 VÜPF

B. Pflichten der FDA mit reduzierten Überwachungspflichten (Art. 51 VÜPF) bei Überwachungen, Notsuchen und Fahndungen

Voraussetzung: FDA bietet Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bereich Bildung und Forschung an (Kriterien gemäss Art. 51 Abs. 1 und 2 VÜPF).

- sind von den Pflichten gemäss Artikel 26 Absatz 1 und 3-5 BÜPF befreit, müssen insbesondere die Überwachungsbereitschaft nicht sicherstellen
- sind vom Pikettdienst befreit gemäss Artikel 11 Absatz 2 VÜPF
- haben lediglich die folgenden Pflichten gemäss Artikel 26 Absatz 2 und 6 BÜPF:
  - die für die Durchführung der Überwachung notwendigen Informationen zu liefern,
  - die Überwachung zu dulden,
  - die von ihnen angebrachten Verschlüsselungen zu entfernen,
  - auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person zu liefern.

C. Pflichten der FDA (normal) bei Auskünften

- erteilen Auskünfte über Fernmeldedienste (Art. 21 BÜPF)
- erteilen Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 BÜPF)
- müssen die Auskunftsbereitschaft sicherstellen (Art. 31 und 32 VÜPF)
- erteilen die Auskünfte aller Typen über die Abfrageschnittstelle des Verarbeitungssystems des Dienstes ÜPF
- erteilen die Auskünfte gemäss den Artikeln 38 und 39 VÜPF
- erteilen die Auskünfte gemäss den Artikeln 35-37 und 40-42 VÜPF sowie gemäss Artikel 27 in Verbindung mit den Artikeln 35, 40 und 42 VÜPF automatisiert
- Aufbewahrungspflichten für die Daten gemäss Artikel 21 Absatz 2 und Artikel 22 Absatz 2 BÜPF sowie Artikel 21 VÜPF
- leisten einen Pikettdienst gemäss Artikel 11 Absatz 2 VÜPF

Erlaubnis:

- können die Auskünfte gemäss den Artikeln 38, 39, 43-48 VÜPF sowie gemäss Artikel 27 in Verbindung mit Artikel 43 VÜPF manuell erteilen

D. Pflichten der FDA (normal) bei Überwachungen, Notsuchen und Fahndungen

- haben die Pflichten gemäss Art. 26 BÜPF:
  - den Inhalt des Fernmeldeverkehrs der überwachten Person zu liefern
  - die Randdaten des Fernmeldeverkehrs der überwachten Person zu liefern
  - die für die Durchführung der Überwachung notwendigen Informationen zu liefern,

  - die Überwachung zu dulden,
  - die von ihnen angebrachten Verschlüsselungen zu entfernen,
  - müssen die Randdaten des Fernmeldeverkehrs während 6 Monaten aufbewahren
- müssen die Überwachungsbereitschaft sicherstellen (Art. 31 und 32 VÜPF)
- leisten einen Pikettdienst gemäss Artikel 11 Absatz 2 VÜPF
- Überwachungspflichten gemäss Artikel 50 VÜPF

E. Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste (normal) bei Auskünften

- müssen dem Dienst ÜPF bei Auskünften zur Identifikation der Täterschaft bei Straftaten über das Internet die ihnen vorliegenden Angaben liefern (Art. 22 Abs. 3 BÜPF)
- sind vom Pikettdienst befreit gemäss Artikel 11 Absatz 2 VÜPF
- sind nicht an die standardisierten Auskunftstypen gebunden, sondern liefern die ihnen vorliegenden Daten formlos (Art. 18 Abs. 4 VÜPF)

F. Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste (normal) bei Überwachungen, Notsuchen und Fahndungen

- haben die Pflichten gemäss Artikel 27 BÜPF:
  - die Überwachung zu dulden (Zugang zu ihren Anlagen zu gewähren und die für die Überwachung notwendigen Auskünfte erteilen),
  - auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person zu liefern
- sind vom Pikettdienst befreit gemäss Arikel 11 Absatz 2 VÜPF

G. Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten (Art. 22 VÜPF) bei Auskünften

Voraussetzung: Anbieterin bietet Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft an (Kriterien gemäss Art. 22 Abs. 1 und 2 VÜPF).

- sind hinsichtlich Auskünfte den "normalen" FDA gleichgestellt
- erteilen Auskünfte über abgeleitete Kommunikationsdienste (Art. 21 BÜPF sinngemäss)
- erteilen Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 BÜPF)
- müssen die Auskunftsbereitschaft sicherstellen (Art. 31 und 32 VÜPF)
- erteilen die Auskünfte aller Typen über die Abfrageschnittstelle des Verarbeitungssystems des Dienstes ÜPF
- sofern sie auch weitergehende Überwachungspflichten haben (Aufbewahrung der Randdaten) erteilen sie die Auskünfte gemäss den Artikeln 38 und 39 VÜPF, sie können sie manuell erteilen
- erteilen die Auskünfte gemäss den Artikeln 35-37 und 40-42 VÜPF sowie gemäss Artikel 27 in Verbindung mit den Artikeln 35, 40 und 42 VÜPF automatisiert
- Aufbewahrungspflichten für die Daten gemäss Artikel 21 Absatz 2 und Artikel 22 Absatz 2 BÜPF sowie Artikel 21 VÜPF
- sind vom Pikettdienst befreit gemäss Artikel 11 Absatz 2 VÜPF

Erlaubnis:

- können die Auskünfte gemäss den Artikeln 43-48 VÜPF sowie gemäss Artikel 27 in Verbindung mit Artikel 43 VÜPF manuell erteilen

H. Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten (Art. 52 VÜPF) bei Überwachungen, Notsuchen und Fahndungen

Voraussetzung: Anbieterin bietet Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft an (Kriterien gemäss Art. 52 Abs. 1 und 2 VÜPF).

- sind den "normalen" FDA hinsichtlich Überwachungen, Notsuchen und Fahndungen gleichgestellt (Art. 27 Abs. 3 BÜPF)
- haben die Pflichten gemäss Artikel 26 Absatz 1-5 BÜPF:
  - den Inhalt des Fernmeldeverkehrs der überwachten Person zu liefern
  - die Randdaten des Fernmeldeverkehrs der überwachten Person zu liefern
  - die für die Durchführung der Überwachung notwendigen Informationen zu liefern,
  - die Überwachung zu dulden,
  - die von ihnen angebrachten Verschlüsselungen zu entfernen,
  - müssen die Randdaten des Fernmeldeverkehrs während 6 Monaten aufbewahren
- müssen die Überwachungsbereitschaft sicherstellen (Art. 31 und 32 VÜPF)
- leisten einen Pikettdienst gemäss Artikel 11 Absatz 2 VÜPF
- Überwachungspflichten gemäss Artikel 50 VÜPF