Entwurf

Verordnung des Bundesministers für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO)

Auf Grund der §§ 94 Abs. 4 und 102c des Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003-TKG 2003), BGBl. I Nr. 70/2003, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 27/2011, wird, hinsichtlich der §§ 1 bis 4 und 8 bis 25 im Einvernehmen mit dem Bundesministerium für Inneres und dem Bundesministerium für Justiz, verordnet:

1. Abschnitt

Allgemeines

Gegenstand und Anwendungsbereich

§ 1. (1) In dieser Verordnung werden die näheren Bestimmungen

1. des Formats, der Datenfelder und der Syntax der CSV-Datei bei der Übermittlung von Auskünften über Verkehrsdaten (§ 99 Abs. 5 TKG 2003) und Vorratsdaten (§ 102b TKG2003),
2. zur Datensicherheit und zur Protokollierung bei der Übermittlung der in Z 1 genannten Auskünfte sowie
3. zur Datensicherheit bei der Speicherung und der Zugriffsprotokollierung von Vorratsdaten

getroffen

(2) Der Anwendungsbereich dieser Verordnung erstreckt sich auf die Verwendung von Verkehrsdaten, Zugangsdaten und Standortdaten sowie Stammdaten, soweit diese in Verbindung mit den eben genannten Datenkategorien verarbeitet werden.

Begriffsbestimmungen

§ 2. (1) Verkehrsdaten, Zugangsdaten und Standortdaten sowie – soweit sie in Verbindung mit den zuvor genannten Datenkategorien verarbeitet werden - Stammdaten werden bezeichnet als

1. „Betriebsdaten“, soweit diese für den Anbieter für die in § 99 Abs. 2 und 3 TKG 2003 erfassten Zwecke notwendig sind;
2. „Vorratsdaten“, soweit diese vom Anbieter ausschließlich aufgrund der Verpflichtung gemäß § 102a TKG 2003 für die in § 102b TKG 2003 genannten Zwecke vorrätig gespeichert werden (§ 92 Abs. 3 Z 6b TKG 2003).

(2) In dieser Verordnung bezeichnet der Begriff

1. „Anbieter“ Betreiber von öffentlichen Kommunikationsdiensten,
2. „Vorratsdatenbank“ eine Datenbank zur Speicherung von Vorratsdaten.

Ausnahmen

§ 3. (1) Die Bestimmungen des 3. Abschnittes sind nicht anzuwenden

1. in den Fällen des § 98 TKG 2003,
2. bei Gefahr in Verzug in den Fällen des § 99 Abs. 5 Z 3 und 4 TKG 2003,
3. bei der Feststellung des aktuellen Standortes gemäß §§ 134 ff der Strafprozessordnung 1975 (StPO), BGBl. Nr. 631 in der Fassung BGBl. I Nr. 33/2011, und

4. bei der Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten.

(2) Anfragen über Verkehrsdaten, Standortdaten und Stammdaten, deren Beantwortung die Verarbeitung von Verkehrsdaten erfordert, einschließlich Anfragen über Vorratsdaten, deren Beantwortung gemäß gesetzlicher Bestimmungen vorab mündlich erfolgen können, müssen mit Ausnahme der Anfragen gemäß § 98 TKG 2003 über die Durchlaufstelle (§ 9) nachgereicht und dokumentiert werden.

Datensicherheitsmaßstab

§ 4. (1) Der Sicherheitsmaßstab bei der Verwendung von Daten im Sinne des § 2 Abs. 1 hat den Vorgaben des § 95 TKG 2003 zu entsprechen.

(2) Bei Verwendung von Vorratsdaten gelten in Ausführung des § 102 Abs. 1 TKG 2003 über Abs. 1 hinaus die im 2. Abschnitt dieser Verordnung ausdrücklich geregelten besonderen Vorschriften für einen erhöhten Sicherheitsmaßstab.

2. Abschnitt

Datensicherheit beim Anbieter innerhalb des Betriebes

Geeignete technische und organisatorische Maßnahmen zur Sicherheit von Vorratsdaten

§ 5. (1) Vorratsdaten müssen vom Anbieter auf eine Weise gespeichert werden, dass deren logische Unterscheidung von Betriebsdaten bei jedem Zugriff und jeder Verwendung eindeutig ist.

(2) Eine physikalisch getrennte Datenspeicherung von Betriebsdaten und Vorratsdaten ist nicht notwendig. Der Anbieter hat durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Vorratsdatenbank auf eine Weise ausgestaltet ist, dass Zugriffe auf Vorratsdaten nur unter Einhaltung der besonderen Sicherheitsvorschriften gemäß § 7 möglich sind.

(3) Wenn keine betriebliche Rechtfertigung zur Speicherung als Betriebsdaten mehr vorliegt, sind diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen. Sollte die Speicherung in der Vorratsdatenbank bereits zuvor gemäß § 6 erfolgt sein, so ist die Kennzeichnung der gleichzeitigen betrieblichen Speicherung zeitgleich oder unmittelbar nach der Löschung aus den betrieblichen Datenbanken zu entfernen.

(4) Der Anbieter hat die Methode zur technischen und organisatorischen Trennung nachvollziehbar zu dokumentieren und diese Dokumentation für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs. 1 TKG 2003 auf Anfrage der Datenschutzkommission zugänglich zu machen.

(5) Der Anbieter hat die tatsächliche Speicherdauer von Betriebsdaten sowie allfällige diesbezügliche interne Richtlinien für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs. 1 TKG 2003 oder auf Anfrage der Datenschutzkommission zu beauskunften.

Unterscheidung von Betriebsdaten und Vorratsdaten

§ 6. (1) Eine Anordnung der Staatsanwaltschaft gemäß § 135 Abs. 2a StPO zur Auskunft über Vorratsdaten berechtigt den Anbieter in jedem Fall zur Erfüllung seiner Auskunftsverpflichtung auch Betriebsdaten zu verarbeiten und zu übermitteln. Die Verpflichtung zur Protokollierung gemäß § 7 Abs. 3 besteht nur dann, wenn der Anbieter zur Erfüllung der Auskunftsverpflichtung tatsächlich eine Abfrage in der Vorratsdatenbank durchführen muss.

(2) Wenn eine Auskunft Vorratsdaten enthält, hat der Anbieter diesen Umstand als Zusatzinformation gemäß der Schnittstellenspezifikation in der Anlage (Kapitel 1.4) zu übermitteln.

(3) Zur Vereinfachung des operativen Betriebes im Hinblick auf Datenauskünfte gemäß § 99 Abs. 5 TKG 2003 oder § 102b TKG 2003 darf der Anbieter die in § 2 Abs. 1 genannten Daten auch dann bereits in der Vorratsdatenbank speichern, wenn diese Daten zugleich noch als Betriebsdaten gespeichert sind. In diesem Fall ist in der Vorratsdatenbank für jede Datenkategorie kenntlich zu machen, dass diese Daten auch in den betrieblich notwendigen Datenbanken des Anbieters vorhanden sind.

Revisionssichere Protokollierung und Vier-Augen-Prinzip bei Zugriffen auf Vorratsdaten

§ 7. (1) Der Anbieter hat seine Systeme auf technischer und organisatorischer Ebene so auszugestalten, dass Zugriffe auf Vorratsdaten nur durch besonders ermächtigte Mitarbeiter unter Einhaltung des Vier-Augen-Prinzips möglich sind. Jeder Zugriff auf Vorratsdaten muss durch zwei Personen mit einer besonderen Ermächtigung hierfür autorisiert sein. Die Autorisierung durch die zweite Person kann auch zeitnah zum Zugriff durch die erste Person nachträglich erfolgen, wenn dabei die effektive Wahrung des Vier-Augen-Prinzips sichergestellt ist.

(2) Zugriffe auf Vorratsdaten müssen beim Anbieter so protokolliert werden, dass die Protokolldaten vor Veränderung und Verfälschung geschützt sind und die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens gewahrt sind.

(3) Die Protokollierung umfasst

1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,
2. in den Fällen des § 99 Abs. 5 Z 3 und 4 TKG 2003 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage (Zustellung in das Postfach des Anbieters in der Durchlaufstelle gemäß § 18 Abs. 1) sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft (Zustellung der Antwort in das Postfach der Behörde in der Durchlaufstelle gemäß § 18 Abs. 3), wobei diese Daten von der Durchlaufstelle als Zusatzinformation an den Anbieter zu übermitteln sind,
4. die nach dem Datum des Beginns des Kommunikationsvorganges und den Kategorien gemäß § 102a Abs. 2 bis 4 TKG 2003 (Einteilung der Kategorien gemäß der Anlage, Kapitel 1.1.2) aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten ab dem Datum, seit dem die Daten als Betriebsdaten (§ 2 Abs. 2 Z 1) und als Vorratsdaten gemäß § 2 Abs. 2 Z 2 gespeichert wurden, zum Zeitpunkt der Anordnung der Auskunft (Datum der staatsanwaltschaftlichen Anordnung gemäß § 138 Abs. 3 StPO oder Datum der Anfrage nach § 53 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991 in der Fassung BGBl. I Nr. 33/2011),
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt,
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben sowie
8. im Fall von Auskünften über Vorratsdaten (§ 135 Abs. 2a StPO) die der Anordnung zu Grunde liegende strafbare Handlung.

3. Abschnitt

Datensicherheit bei der Übermittlung von betriebsnotwendigen Verkehrs- und Standortdaten und Vorratsdaten zu Auskunftszwecken an Strafverfolgungs- und Sicherheitsbehörden

Allgemeines

§ 8. (1) Die Übermittlung der Daten erfolgt über eine zentrale Durchlaufstelle, die das Bundesministerium für Verkehr, Innovation und Technologie bei der Bundesrechenzentrum GmbH einzurichten hat.

(2) Die technische Spezifikation zur Durchlaufstelle hat einen verschlüsselten Übertragungsweg vorzusehen (Transportverschlüsselung).

(3) Zusätzlich ist eine Verschlüsselung der Inhalte sowohl der Anfrage als auch der Beantwortung von Absender zu Empfänger durch asymmetrische Verschlüsselungsverfahren vorzusehen (Inhaltsverschlüsselung). Asymmetrische Verschlüsselungsverfahren können als hybride Verfahren implementiert werden.

(4) Über die Durchlaufstelle werden die Teilnehmer des Datenaustausches über eine fortgeschrittene elektronische Signatur identifiziert und authentifiziert.

Durchlaufstelle – Grundstruktur

§ 9. (1) Die Durchlaufstelle ist ein elektronisches Postfachsystem zur sicheren Abwicklung von Anfragen und Auskünften im Sinne des § 94 Abs. 4 TKG 2003. Alle Beteiligten sind dabei über einen verschlüsselten Übertragungskanal an die Durchlaufstelle angebunden.

(2) Die Durchlaufstelle ist auf eine Weise einzurichten, dass für die Bundesrechenzentrum GmbH als Dienstleister der Durchlaufstelle im Sinn des DSG 2000 ein Zugang zu personenbezogenen Inhalten von Anfragen zu Datenauskünften so wie von deren Beantwortung nicht möglich ist.

(3) Über die Durchlaufstelle werden sowohl Auskünfte über Vorratsdaten als auch Auskünfte über Betriebsdaten abgewickelt. Ausnahmen sind nur in dem von § 3 normierten Ausmaß zulässig. Über die Durchlaufstelle werden alle Auskunftsfälle revisionssicher statistisch erfasst.

(4) In der Spezifikation zur Durchlaufstelle ist vorzusehen, dass die Integrität der Daten sowie die Identität des Senders durch den Empfänger überprüft werden kann (Signatur).

Einrichtung und Betrieb der Durchlaufstelle – Auftraggeber und Durchführung

§ 10. (1) Die Einrichtung der Durchlaufstelle sowie die Zertifikatsverwaltung und die Datensicherheit liegen in der Verantwortung des Bundesministeriums für Verkehr, Innovation und Technologie.

(2) Die Einrichtung, die Zertifikatsverwaltung und der Betrieb der Durchlaufstelle erfolgen durch die Bundesrechenzentrum GmbH. Die Bundesrechenzentrum GmbH ist funktionell Dienstleister im Sinne des § 4 Z 5 DSG 2000 jeweils für den Auftraggeber, für dessen Anwendung Daten an die Durchlaufstelle übergeben oder von der Durchlaufstelle übernommen werden.

(3) Der Bundesminister für Verkehr, Innovation und Technologie kann sich zur Auditierung der tatsächlichen Umsetzung der technischen Spezifikation durch die Bundesrechenzentrum GmbH eines Dienstleisters bedienen.

Auditierung der Durchlaufstellen-Funktionen

§ 11. Der Bundesminister für Verkehr, Innovation und Technologie stellt sicher, dass

1. die tatsächliche Umsetzung der Durchlaufstelle durch die Bundesrechenzentrum GmbH den Spezifikationen zur Durchlaufstelle entspricht,
2. jene Dienste, die von der Durchlaufstelle für die Ausführung in der Client-Software der jeweiligen Benutzer zur Verfügung gestellt werden, für einen Client-Administrator verifizierbar ist (Signatur) und der Schnittstellendefinition zur Durchlaufstelle entspricht,
3. nur eine auditierte schnittstellenkonforme Software der Durchlaufstelle eine richtige Datenübertragung ermöglicht,
4. nur authentifizierte Anwender ihre öffentlichen Schlüssel in der Durchlaufstelle eindeutig zu ihrer jeweiligen Institution zugehörig hinterlegen können und
5. jede Änderung der Durchlaufstelle einer Re-Auditierung zum Zweck der Sicherstellung der Verifizierbarkeit der Echtheit der Software durch die Endnutzer unterliegt.

Funktionen der Durchlaufstelle im Überblick

§ 12. (1) Die Durchlaufstelle stellt für die Abwicklung von Auskünften im Sinne des § 94 Abs. 4 TKG 2003 elektronische Postfächer zur Verfügung, die unter Verwendung eines Webservice oder einer Webapplikation zu benutzen sind.

(2) Allen zur Abwicklung von Auskunftsbegehren ermächtigten Dienststellen auf Seiten der berechtigten Behörden sowie allen nach § 102a TKG 2003 speicherpflichtigen Anbietern wird jeweils eine Teilnehmerkennung und ein dazugehöriges Postfach von der Durchlaufstelle zugewiesen. Jeder Benutzer hat nur Zugriff auf das Postfach jenes Teilnehmers (Dienststelle oder Anbieter), dem der Benutzer zugehört.

(3) Die Authentifizierung der Benutzer erfolgt durch die Durchlaufstelle gemäß den Vorgaben des § 13.

(4) Die Verschlüsselung des Übertragungsweges ist über die Durchlaufstelle unter Verwendung einer geeigneten Technologie entsprechend dem Stand der Technik sicherzustellen.

(5) Zur Verschlüsselung der Anfragen und der Auskünfte verwaltet die Durchlaufstelle die öffentlichen Schlüssel aller ermächtigten Dienststellen und aller gemäß § 102a TKG 2003 speicherpflichtigen Anbieter. Nur authentifizierte Benutzer können den öffentlichen Schlüssel ihrer Organisation bei der Durchlaufstelle hinterlegen. Jeder Benutzer holt vor dem Absenden seiner Nachricht den öffentlichen Schlüssel des Empfängers zur Verschlüsselung des Inhalts bei der Durchlaufstelle ab.

(6) Alle Auskunftsfälle sind in der Durchlaufstelle revisionssicher zu protokollieren. Der Umfang dieser Protokollierung wird in § 23 geregelt.

Authentifizierung – Einbindung über den Portalverbund und Unique-ID

§ 13. (1) Die Durchlaufstelle vergibt zu jeder Anfrage eine einmalige, eindeutig zuordenbare Transaktionsnummer zur Prüfung der Authentizität der Anfrage und zur Nachverfolgung jeder Anfrage sowie deren Beantwortung (Unique-ID). Aus der Transaktionsnummer muss sowohl auf die zugrunde liegende konkrete Anfrage der Behörde als auch auf den angefragten Betreiber geschlossen werden können.

(2) Die Authentifizierung der Benutzer der berechtigten Behörden erfolgt durch das jeweilige Stammportal des Benutzers (Portalverbund).

(3) Für die Authentifizierung der Benutzer auf Seiten der Anbieter ist in der Spezifikation zur Durchlaufstelle ein Stammportal vorzusehen, das der Sicherheitsklasse 3 der Portalverbundvereinbarung entspricht.

Zugangsberechtigte Behörden

§ 14. (1) Das Bundesministerium für Inneres sowie das Bundesministerium für Justiz geben der Bundesrechenzentrum GmbH für die Spezifikation der Durchlaufstelle eine begrenzte Anzahl von Dienststellen bekannt, die als Teilnehmer der Durchlaufstelle zur Abwicklung von Auskunftsbegehren berechtigt sind.

(2) Nachträgliche Änderungen der nach Abs. 1 bekannt gegebenen Dienststellen sind durch das Bundesministerium für Inneres sowie das Bundesministerium für Justiz der Bundesrechenzentrum GmbH für die Veranlassung der entsprechenden Änderungen in der Durchlaufstelle bekannt zu geben.

(3) Für die Datenschutzkommission, den Datenschutzrat und das Bundesministerium für Justiz sowie für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und beim Bundesminister für Inneres ist in der Spezifikation zur Durchlaufstelle jeweils ein Zugang vorzusehen, der entsprechend der jeweiligen Aufgabe dieser Stellen einen Zugang zu den Protokolldaten gemäß § 22 Abs. 4 oder zur Statistik gemäß § 23 Abs. 3 ermöglicht.

Anbindung der Anbieter

§ 15. (1) Die Anbindung an die Durchlaufstelle ist für alle Anbieter verpflichtend, die gemäß § 102a Abs. 6 TKG 2003 zur Vorratsdatenspeicherung verpflichtet sind. Die Erfassung aller speicherpflichtigen Anbieter zur erstmaligen Einrichtung des Stammportals der Anbieter gemäß § 13 Abs. 3 erfolgt durch die Rundfunk und Telekom Regulierungs-GmbH, welche der Bundesrechenzentrum GmbH eine Liste aller erfassten Anbieter zur Importierung und Freigabe zur Verfügung stellt.

(2) Entsteht ein neuer speicherpflichtiger Anbieter oder fällt ein bestehender weg, hat die Rundfunk und Telekom Regulierungs-GmbH alle notwendigen Informationen über diesen Anbieter der Bundesrechenzentrum GmbH für die Freigabe oder zur Deaktivierung der Anbindung an die Durchlaufstelle bekannt zu geben.

Sicherheitsniveau der Anbindung

§ 16. (1) Die Anbindung der Behörden an die Durchlaufstelle hat den Vorgaben der Sicherheitsklasse 3 in der Portalverbundvereinbarung zu entsprechen.

(2) Die Anbindung der Anbieter an die Durchlaufstelle hat den Vorgaben der Sicherheitsstufe 3 aus der Definition der Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich E-Government zu entsprechen.

Postfächer und Zustellung

§ 17. (1) Ein Auskunftsbegehren eines berechtigten Benutzers auf Behördenseite wird in das Postfach des über die Durchlaufstelle ausgewählten Anbieters zugestellt. Die Durchlaufstelle ermöglicht die Auswahl mehrerer Anbieter. Die Spezifikation zur Durchlaufstelle hat ein System der Notifikation über den Eingang eines Auskunftsbegehrens in das Postfach des Anbieters vorzusehen. Die Abholung des Auskunftsbegehrens erfolgt manuell durch Zugriff auf das Postfach des Anbieters nach entsprechender Authentifizierung des Benutzers. Eine Abholung des Auskunftsbegehrens per Webservice kann in der Spezifikation zur Durchlaufstelle vorgesehen werden.

(2) In der Spezifikation zur Durchlaufstelle muss sichergestellt werden, dass eine Beantwortung bereits vor der Übermittlung der Anfrage via Durchlaufstelle durchgeführt werden kann. Dazu wird ein anbieterspezifischer Bereich von Referenzen (Unique-ID) definiert, der vom Anbieter in aufsteigender Reihenfolge vergeben wird. Gemäß § 3 Abs. 2 ist die nachträgliche Dokumentation der Anfrage über die Durchlaufstelle zu gewährleisten, wobei die Behörde die anbieterspezifische Referenz anzugeben hat, die bei der Beantwortung verwendet wurde.

(3) Die Beantwortung eines Auskunftsbegehrens durch den Anbieter erfolgt durch Übermittlung einer verschlüsselten CSV-Datei gemäß der Schnittstellenspezifikation in der Anlage zu dieser Verordnung. Die Durchlaufstelle stellt automatisch sicher, dass die Antwort in das richtige Postfach der anfragenden Dienststelle zugestellt wird. In den Fällen des Abs. 2 muss die adressierte Dienststelle jedoch durch individuelle Auswahl über die Durchlaufstelle bestimmt werden.

(4) Die Durchlaufstelle versendet nach Eingang der Antwort in das Postfach der anfragenden Dienststelle eine Benachrichtigung über die Hinterlegung der Antwort an die Dienststelle.

(5) Die Abholdung der Auskunft erfolgt manuell durch Zugriff auf das Postfach der Dienststelle nach entsprechender Authentifizierung des Benutzers. Eine Abholung der Auskunft per Webservice kann in der Spezifikation zur Durchlaufstelle vorgesehen werden.

Verschlüsselung/Signatur der Antwort

§ 18. (1) Die vertrauenswürdige Stelle zur Hinterlegung der Zertifikate ist das Bundesministerium für Verkehr, Innovation und Technologie, das diese Funktion über die Durchlaufstelle technisch wahrnimmt. Jeder Teilnehmer kann in der Durchlaufstelle nur zu seiner Institution zugehörige eindeutige Schlüssel hinterlegen.

(2) Die Echtheit der Software, die von der Durchlaufstelle zur Verschlüsselung durch den Client zur Verfügung gestellt wird, muss für einen Client-Administrator eindeutig verifizierbar sein. Die Verschlüsselung und die Signatur erfolgt auf Client Seite, nur der öffentliche Schlüssel wird bei der Durchlaufstelle abgeholt.

(3) In der Spezifikation zur Durchlaufstelle ist eine eindeutige Definition der Dateinamen für die Übermittlung der Antwort sowie der Signatur zur Verschlüsselung der Dateien vorzunehmen. Es ist eine fortgeschrittene elektronische Signatur im Sinne des § 2 Z 3 des Signaturgesetzes, BGBl. I Nr. 190/1999 in der Fassung BGBl. I Nr. 75/2010, vorzusehen.

(4) Wenn die Antwort aus mehreren CSV-Dateien besteht, ist es optional möglich, alle Dateien zu einer Abfrage zu einer Gesamtdatei zusammenzufassen. Die Gesamtdatei kann optional komprimiert werden. Die komprimierte oder unkomprimierte Gesamtdatei ist für die Übermittlung zu verschlüsseln, nicht aber die einzelnen Dateien.

Eingabefelder

§ 19. (1) Über die Durchlaufstelle ist bei jeder Anfrage auszuwählen, ob es sich um ein Auskunftsbegehren nach § 53 Abs. 3a SPG, nach § 53 Abs. 3b SPG, nach § 76a StPO, nach § 135 Abs. 2 StPO oder nach § 135 Abs. 2a StPO oder um eine Stammdatenauskunft nach § 21 handelt. In der Durchlaufstelle ist ein Feld für den Eintrag der einer Anordnung zu Grunde liegenden strafbaren Handlung für die Protokollierung gemäß § 7 Abs. 3 Z 8 vorzusehen. Eine allfällige Eingabemaske auf Behördenseite kann unter Beachtung der Schnittstellenspezifikation in der Anlage frei gestaltet werden.

(2) Dies gilt sinngemäß auch für eine allfällige Eingabemaske auf Anbieterseite. Insbesondere besteht keine Verpflichtung zur automatisierten Befüllung der CSV-Datei.

Zusatzinformationen

§ 20. Die Durchlaufstelle hat die Übertragung von Zusatzinformationen zu unterstützen. Zusatzinformationen können allenfalls über ein Web-Interface zu der entsprechenden Abfrage eingegeben werden. Diese Zusatzinformationen könnten auch Gründe für eine Leer-Meldung beschreiben. Ob und in welchem Ausmaß ein Web-Interface auf Seiten der Durchlaufstelle zur Verfügung gestellt werden soll, ist in der Spezifikation zur Durchlaufstelle zu regeln. Voraussetzung ist in jedem Fall, dass die Durchlaufstelle keinen Zugang zu personenbezogenen Inhalten der Auskünfte hat.

Optionale Stammdatenauskünfte über die Durchlaufstelle

§ 21. Anbieter und zugangsberechtigte Behörde können jeweils im Einvernehmen optieren, Stammdatenauskünfte über die Durchlaufstelle abzuwickeln. Die technischen Details solcher Auskünfte sind in der Spezifiktion zur Durchlaufstelle zu regeln.

Protokollierung über die Durchlaufstelle

§ 22. (1) Die Protokollierung der Durchlaufstelle enthält keine personenbezogenen Daten. Durch die Unique-ID jeder Anfrage wird der Zusammenhang zwischen jeder Anfrage und deren Beantwortung ohne Personenbezug hergestellt.

(2) Bei der Übermittlung der Antwort zu einem Auskunftsbegehren hat der Anbieter die Protokollinformationen gemäß § 7 Abs. 3 Z 4 und 5 für die in Abs. 4 genannten Zwecke an die Durchlaufstelle zu übermitteln.

(3) Die Protokolldaten werden in einer Protokolldatei unverschlüsselt über die sichere Transportverbindung zur Durchlaufstelle übermittelt. Das Format der Datei und der Dateiname sind in der Spezifikation zur Durchlaufstelle festzulegen.

(4) Die Protokolldaten sind ausschließlich für die definierten Protokolldatenempfänger zugänglich und werden innerhalb der Durchlaufstelle in einer gesonderten Datenbank archiviert. Für die Datenschutzkommission sowie für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und

beim Bundesminister für Inneres sind in der Spezifikation zur Durchlaufstelle gesonderte Berechtigungen für den Zugang zu den Protokolldaten vorzusehen.

Statistik aus den Protokolldaten

§ 23. (1) Die Statistik zur Erfüllung der Verpflichtung aus Art. 10 der Richtlinie 2006/24/EG soll in der Durchlaufstelle automatisch aufbereitet werden. Die genaue Definition der zu erstellenden Statistik ist in der Spezifikation zur Durchlaufstelle vorzunehmen.

(2) Für die Erstellung der Statistik sind die Protokoll-Informationen gemäß § 7 Abs. 3 Z 3 bis 5 und Z 8 erforderlich. Die Informationen gemäß § 7 Abs. 3 Z 3 sind von der Durchlaufstelle automatisch zu jedem Auskunftsfall zu erfassen. Die Informationen gemäß § 7 Abs. 3 Z 4 und 5 hat der Anbieter gemäß § 23 Abs. 2 gemeinsam mit der Beantwortung des Auskunftsbegehrens an die Durchlaufstelle zu übermitteln.

(3) Zugang zur Statistik der Durchlaufstelleerhalten gemäß § 102c Abs. 4 TKG 2003 das Bundesministerium für Justiz, der Datenschutzrat, und die Datenschutzkommission. Darüber hinaus ist in der Spezifikation zur Durchlaufstelle ein elektronischer Zugang für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und beim Bundesminister für Inneres vorzusehen.

Kostentragung der Durchlaufstelle

§ 24. Die Investitionskosten für die Durchlaufstelle sind Investitionskosten gemäß § 94 Abs. 1 TKG 2003.

4. Abschnitt

Definition Syntax und Semantik der CSV-Datei für Auskünfte

Schnittstellendefinition EP020

§ 25. Die Schnittstellendefinition ergibt sich aus der Anlage.

Erläuterungen

Allgemeiner Teil

Die Verordnungsermächtigungen der §§ 94 Abs. 4 und 102c TKG 2003 werden gegenständlich mit einer einheitlichen Verordnung geregelt. Diese Verordnung wird von der Bundesministerin für Verkehr, Innovation und Technologie erlassen, wobei jene Teile der Verordnung, die in Ausführung des § 94 Abs. 4 TKG 2003 ergehen, im Einvernehmen mit dem Bundesminister für Inneres und dem Bundesminister für Justiz zu erlassen sind, während ein solches Einvernehmen in Bezug auf die § 102c TKG ausführenden Bestimmungen nicht erforderlich ist. Letzteres betrifft die Bestimmungen im 2. Abschnitt (§§ 5 bis 7), wobei auch zu diesen in der Vorbreitung grundsätzliches Einvernehmen hergestellt wurde.

Besonderer Teil

Zu § 1:

In den Erläuterungen zu § 94 Abs. 4 TKG 2003 wird der Spielraum abstrakt beschrieben, den der Verordnungsgeber bei der Ausgestaltung dieser Bestimmung hat: „Die Bestimmung identifiziert die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten. Die Übertragungstechnologie, welche durch eine Verordnung („Technische Richtlinie“) nach dieser Bestimmung zu konkretisieren ist, soll durch sichere „Identifikation und Authentifizierung von Sender Empfänger“ sicherstellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden, Staatsanwaltschaften und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht. Dabei muss auf technischer Ebene die Datenintegrität gewahrt sein. Das bedeutet, dass jede allfällige Veränderung der übermittelten Daten auf dem Übertragungsweg für den Empfänger sofort identifizierbar wäre und dieser sich damit auf die Richtigkeit der Daten nicht mehr verlassen darf. Die Formulierung „unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie“ (im Gegensatz zur Fassung im ursprünglichen Begutachtungsentwurf vom Dezember 2009 „Übertragung per E-Mail“) ist eine Ergänzung zur Erfüllung anspruchsvoller Datensicherheitsstandards, wie sie insbesondere im Urteil des deutschen Bundesverfassungsgerichts zu BVerfG, 1 BvR 256/08 vom 2.3.2010 beschrieben werden. Die Formulierung lässt genügend Spielraum, die nähere technische Ausgestaltung durch Verordnung zu regeln und stellt gleichzeitig einen Auftrag an den Verordnungsgeber dar. Die gesetzlich vorgezeichneten Indikatoren sind dabei technologieneutral formuliert. Wesentlich ist, dass die eingesetzte Technologie den Zielvorgaben entspricht.

Am 7.4.2011 wurde die TKG Novelle zur Umsetzung der Vorratsdatenspeicherung im Ausschuss für Forschung, Innovation und Technologie (FIT Ausschuss) des Nationalrats diskutiert (siehe dazu den Ausschussbericht: 1157 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV. GP). In diesem Rahmen wurde ein Antrag für eine Ausschussfeststellung zum Thema Datensicherheit eingebracht, der eine Grundsatzerklärung für die Implementierung der Durchlaufstelle enthält. Diese Ausschussfeststellung wurde mit den Stimmen der Regierungsfraktionen angenommen und lautet wie folgt: „Für die Datensicherheit und die Nachvollziehbarkeit der Zugriffe auf den Datenvorrat ist das Zusammenspiel der Bestimmungen der §§ 94 Abs. 4 und 102c TKG von besonderer Bedeutung. Während § 94 Abs. 4 TKG 2003 den Aspekt der technischen Datenintegrität und der Determinierung der Verordnungsermächtigung über die Art der Verschlüsselung betrifft und die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten identifiziert, um durch sichere ‚Identifikation und Authentifizierung von Sender und Empfänger‘ sicherzustellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden, Staatsanwaltschaften und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht, regelt § 102c TKG 2003 Zugriffs- und Sicherheitsbestimmungen. Einerseits muss jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein, um zu gewährleisten, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Andererseits müssen Zugriffe auf Vorratsdaten beim Anbieter revisionssicher protokolliert werden. Die wichtigsten Kriterien sind dabei der Schutz vor Veränderung und Verfälschung, die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens, wozu etwa bei Anordnungen der Staatsanwaltschaft auch die Angabe der Geschäftszahl der ermittelnden Kriminalpolizei zählt. Der Ausschuss geht davon aus, dass sämtliche Zugriffe und Übermittlungen von wem auch immer auf Vorratsdaten gemäß § 94 Abs. 4 TKG lückenlos protokolliert werden. Der Ausschuss geht weiters davon aus, dass ein automatisches zentrales System der Protokollierung solcher Abfragen und Übermittlungen notwendig ist, wobei unter dieser Protokollierung nicht die in § 102c Abs. 2 TKG 2003genannte zu verstehen ist. Sie wird vielmehr

nur jene Daten umfassen, die zur statistischen Auswertung und zur Verknüpfung mit der gemäß § 102c Abs. 2 TKG 2003 erfolgenden Protokollierung dient. Wünschenswert ist die Einrichtung einer ‚Datendrehscheibe' (‚Durchlaufstelle', kurz: DLS). Da jeder Auskunftsfall über die DLS mit einer fortlaufenden einmaligen Nummer versehen wird, kann im Falle einer Nachprüfenden Kontrolle über die Protokollierung bei der DLS zur Protokollierung beim Anbieter gemäß § 102c Abs. 2 TKG 2003 verknüpft werden. Zugang zu den übermittelten personenbezogenen Daten soll die DLS selbst nicht bieten, die Daten liegen dort nur verschlüsselt bis zur Abholung bereit und werden bei der Abholung automatisch gelöscht."

Festzuhalten ist, dass diese Ausschussfeststellung sachlich auf der gemeinsamen Arbeit zur Entwicklung der Schnittstellenbeschreibung und eines sicheren Systems der Datenübermittlung in den Round Table Diskussionen basiert, die das Ludwig Boltzmann Institut für Menschenrechte (BIM) im Rahmen einer Studie zur Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung im Auftrag des BMVIT ausgearbeitet hat. Die Ausschussfeststellung bezieht sich auf den Diskussions- und Einigungsstand beim 3. von insgesamt 6 Round Table Veranstaltungen am 24.3.2011, bei dem die Grundsatzeinigung auf das Konzept der Durchlaufstelle (siehe § 10) bereits Konsens unter allen Beteiligten war.

Zu § 1 Abs. 2:

Zunächst wird klargestellt, dass diese Verordnung nicht ausschließlich Vorratsdaten betrifft. Soweit es nämlich um die Übermittlung von Verkehrsdaten, Zugangsdaten und Standortdaten für Auskünfte gegenüber Sicherheits- und Strafverfolgungsbehörden geht, die beim Anbieter für betriebliche Zwecke gespeichert sind, sind die Datensicherheitsvorschriften auch für diese Daten relevant. Hinsichtlich jener Bestimmungen, die Datensicherheitsmaßen innerhalb des Betriebes des Anbieters betreffen, ist die Verordnung allerdings nur für Vorratsdaten maßgeblich, denn nur für diese gelten gemäß § 102c TKG 2003 die strengen Zugriffsbestimmungen. Ansonsten gilt der allgemeine Sicherheitsmaßstab, den das TKG 2003 und das DSG 2000 vorgeben (siehe dazu die Erläuterungen zu § 4).

Schließlich wird bewusst die Formulierung „Verwendung" normiert. Nach § 4 Z 8 DSG 2000 ist „Verwenden von Daten" definiert wird als „ jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten" und der Begriff „Verarbeiten von Daten" gemäß § 4 Z 9 DSG 2000 auch die Speicherung umfasst. In der österreichischen datenschutzrechtlichen Terminologie ist dies der weiteste Begriff, der alle Fälle möglicher Datenverwendungen - insbesondere die Übermittlung von Daten - umfasst. Weil gerade im Regelungsbereich des § 94 Abs. 4 TKG 2003 die Übermittlung im Vordergrund steht, wird hier der Rechtsbegriff der Datenverwendung nutzbar gemacht. Aus dem Regelungsumfang der Verordnung ist zugleich klar, dass die weitere Verwendung der betreffenden Daten nach der Übermittlung über die DLS - insbesondere die weitere Verwendung der Daten für die Zwecke der Strafverfolgung - nicht von dieser Verordnung bestimmt wird.

Zu § 2 Abs. 1:

Diese Bestimmung definiert die Bezeichnung der beiden Datenarten, deren Unterscheidung vom Zweck der Verarbeitung und Speicherung abhängt. An diese Unterscheidung sind einige rechtliche Konsequenzen geknüpft, die durch eine Konkretisierung und klare Formulierung der an sich schon im TKG 2003 vorgezeichneten Definitionen leichter normativ zu erfassen sind. In Z 1 wird bewusst der Begriff „Betriebsdaten" eingeführt, weil in zahlreichen öffentlichen Diskussionen zum Thema Vorratsdatenspeicherung oft nur der Begriff der „Verrechnungsdaten" verwendet wird, der jedoch zu kurz greift. Wohl bilden die Daten zum Zweck der Rechnungslegung (§ 99 Abs. 2 TKG 2003) den praktisch wichtigsten Fall, doch auch jene Daten, die beim Anbieter zum Zweck der Aufrechterhaltung des Betriebes und insbesondere der technischen Wartung der Betriebsanlagen (§ 99 Abs. 3 TKG 2003) verarbeitet und gespeichert werden, sind nach der bisherigen Rechtslage vor Umsetzung der Vorratsdatenspeicherung regelmäßig Gegenstand von behördlichen, staatsanwaltschaftlichen und gerichtlichen Auskunftsersuchen. Z 2 gibt die Legaldefinition des § 92 Abs. 3 Z 6b TKG 2003 wieder und verbindet diese mit der Zweckwidmung des § 102b TKG 2003. Damit soll lediglich die strenge Zweckbindung, die nur durch die Ausnahmen in § 99 Abs. 5 TKG 2003 durchbrochen wird, eindeutig klargestellt werden, ein über die Definition im TKG 2003 hinausgehender normativer Gehalt entsteht daraus nicht.

Zu § 3 Abs. 1:

Absatz 1 nimmt jene Fälle vom Datensicherheitsregime des 3. Abschnitts dieser Verordnung aus, die bereits durch die gesetzliche Regelung des § 94 Abs. 4 TKG 2003 als Ausnahmen vorgesehen sind. Aufgezählt werden jene Fälle, in denen eine Beantwortung von Auskunftsbegehren durch den Anbieter nach einem anderen Regime vorgesehen oder zumindest zulässig ist und keine Verschlüsselung nach dem 3. Abschnitt zwingend durchzuführen ist. Die auf § 98 TKG 2003 bezogene Ausnahme bezieht sich auf die Identifizierung und Lokalisierung von Anschlüssen bzw. Endgeräten, von denen ein Notruf abgesetzt

wurde. Für diese Fälle wird es künftig nach der Umsetzung des neuen Telekom Rechtsrahmens eine eigene Schnittstelle geben, um eine sofortige Reaktion der Notrufträger zu ermöglichen, wobei damit eine automatische nachträgliche Information der Betroffenen verbunden ist. Die Umsetzung dieser gemeinschaftsrechtlichen Verpflichtung steht unmittelbar bevor, daher ist dieser Fall aus dem Anwendungsbereich dieser Verordnung ausgeklammert.

Die Fälle des § 99 Abs. 5 Z 3 und 4 TKG 2003 bei Gefahr im Verzug gemäß Z 2 bezieht sich auf Anfragen nach § 53 Abs. 3a und 3b SPG, wenn aufgrund der besonderen Umstände des Falles der Zweck der Auskunft (zB die Abwehr einer gegenwärtigen oder unmittelbar drohenden Gefahr) dadurch gefährdet wäre, dass die Abwicklung der Auskunft über das System der DLS zu lange dauern würde und daher eine schnellere Form der Beauskunftung unerlässlich ist, zB eine telefonische Auskunft über die Standortdaten des Endgerätes einer akut gefährdeten Person. Die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten erfolgt über die ETSI Schnittstelle zur Inhaltsüberwachung durch Übergabe der sogenannten „S-Records".

Zu § 3 Abs. 2:

Absatz 2 dieser Bestimmung regelt die gesetzlich definierten Ausnahmefälle für Anfragen abseits der DLS sowie die Verpflichtung zur nachträglichen Dokumentation über die DLS. Ganz generell ist hier voraus zu schicken, dass das Konzept der DLS auch darauf abzielt, die Abwicklung von Auskunftsbegehren im Vergleich zur bisherigen Praxis (Fax- und E-Mail- Anfragen) zu beschleunigen und den Verwaltungsaufwand sowohl auf Behörden- als auch auf Anbieterseite zu reduzieren. Es ist daher nicht generell davon auszugehen, dass eine Abwicklung abseits der DLS tatsächlich jene Beschleunigung mit sich bringt, welche die gesetzlichen Ausnahmen rechtfertigen soll. Die Praxis ab dem Vollbetrieb des neuen Konzepts ab 1.4.2012 wird zeigen, ob gerade in dringenden Fällen eine Abwicklung über die DLS nicht sogar vorteilhaft sein wird. Die technische Spezifikation sollte hierzu also jedenfalls den Usecase "nachträgliche Anfragedokumentation" berücksichtigen und idealer weise auch eine Prioritäteninformation bei der Notifikation über die DLS vorsehen. Bereits die Erläuterungen zu § 94 Abs. 4 TKG 2003 führen zu den Ausnahmen aus: „Ausdrücklich gesetzlich gefordert ist eine Verschlüsselung bei der Übermittlung. Davon ausgenommen sein soll die Übermittlung von Daten in Notfällen. In diesen Fällen soll daher die bisher praktizierte Übermittlungsform beibehalten werden, also Auskünfte per Telefon oder Fax. Die weiteren Ausnahmen vom Grundsatz der Übermittlung in einem CSV-File berücksichtigen die in der Praxis wichtigen Fälle, in denen aufgrund der besonderen Dringlichkeit (insbesondere bei Standortdatenauskünften, etwa zur Lebensrettung oder bei zeitkritischen Observationen) dieses Verfahren nicht zweckmäßig wäre. Außerdem sind die sogenannten „S-Records" (das sind die begleitenden Verkehrsdaten bei einer Inhaltsüberwachung von Telefongesprächen) berücksichtigt, welche über eine besondere technische Schnittstelle gemeinsam mit der Inhaltsüberwachung abgewickelt werden."

Die in den Ausnahmen genannten Fälle des § 99 Abs. 5 Z 3 und 4 TKG 2003 betreffen Auskünfte nach § 53 Abs. 3a und Abs. 3b SPG, bei denen eine Anfrage bzw. Beantwortung via DLS bei Gefahr in Verzug unterbleiben kann. Standortdatenanfragen nach § 53 Abs. 3b SPG werden dabei schon aufgrund des dort normierten Tatbestandes (Abwehr einer „gegenwärtigen Gefahr" für den Inhaber der Endeinrichtung) regelmäßig einen Fall von „Gefahr in Verzug" darstellen. Festzuhalten ist, dass in diesen Fällen nur ausnahmsweise überhaupt historische Standortdaten begehrt werden, nämlich nur dann, wenn eine live-Ortung (durch sog. „stummes SMS") erfolglos bleibt, etwa weil das Endgerät defekt oder ausgeschaltet ist. In Fällen von Gefahr im Verzug kann die Anfrage telefonisch übermittelt werden. Es erfolgt eine Nachreichung der Anfrage über die DLS, wobei davon auszugehen ist, dass die Beantwortung der Anfrage bereits vor der Nachreichung der Anfrage erfolgt. Dies bedeutet, dass bei der technischen Spezifikation der DLS Festlegungen zur Unique-ID getroffen werden müssen. Dazu könnte jedem Anbieter ein eigener Bereich von Referenznummern zugeteilt werden. Der Anbieter verwendet diese Referenznummern in aufsteigender Reihenfolge im Falle, dass die betreffende Anfrage noch nicht über die DLS eingelangt ist. In der Durchlaufstelle muss dann die Zuordnung zwischen Anfrage und (bereits erfolgter) Durchführung erfolgen. Es ist hier nur der Usecase "nachträgliche Anfragedokumentation" zu berücksichtigen (Daten wurden bereits übermittelt) + Übermittlung von Protokolldaten bei Zugriff auf Vorratsdaten.

SPG Anfragen können

a) bei Gefahr im Verzug

- mündlich
- lt. SPG von jeder Sicherheitsbehörde
- schriftlich

- oder über die DLS

b) wenn keine Gefahr im Verzug vorliegt

- durch Anfrage (und Antwort) über die DLS

zum Anbieter gelangen.

Die Dokumentation über die DLS ist dabei sinnvoll und notwendig, da teilweise (insbesondere bei Anfragen zu IP-Adressen und E-Mail Daten) auch Vorratsdaten betroffen sein werden und der Anbieter bei Zugriff auf Vorratsdaten die Protokolldaten gemäß § 7 Abs. 3 Z 3 bis 5 zu übermitteln hat und der besondere Rechtsschutz (Informationspflicht der Behörde) ausgelöst wird.

Auch im Rahmen von StPO-Abfragen kann es - eng begrenzte - Fälle geben, in denen eine mündliche Übermittlung der Anordnung erfolgt. Anordnungen von Zwangsmaßnahmen sind von der Staatsanwaltschaft begründet und schriftlich auszufertigen und an die Kriminalpolizei zu richten. In dringenden Fällen kann aber eine solche Anordnung vorläufig mündlich übermittelt werden (§ 102 Abs. 1 StPO). Dies gilt auch für die Anordnung einer „Auskunft über Daten einer Nachrichtenübermittlung“ (§ 134 Z 2 StPO) sowie künftig bei einer „Auskunft über Vorratsdaten“ (§ 134 Z 2a StPO). In dringenden Fällen kann eine solche mündliche Anordnung auch auf Grund einer mündlichen gerichtlichen Bewilligung (§ 105 StPO) erteilt werden. So kann im Fall des § 135 Abs. 2 Z 1 StPO (noch andauernde Entführung) eine Dringlichkeit vorliegen, die zumindest erfordert, dass die Übermittlung des Auskunftsbegehrens vorerst „auf kürzestem Weg“ an den Anbieter gerichtet wird, während die Antwort über die sichere Verbindung gemäß § 94 Abs. 4 TKG 2003 übermittelt werden muss, weil diesbezüglich keine gesetzliche Ausnahme vorgesehen ist. Aus Sicht des TKG 2003 ist dies rechtlich zulässig, da § 94 Abs. 4 TKG 2003 ausdrücklich nur die Beantwortung, aber nicht die Übermittlung der Anordnung regelt. Diesbezüglich wäre gemäß § 102 Abs. 1 StPO die schriftliche und begründete Anordnung der Staatsanwaltschaft nachzureichen. Das Erfordernis einer gerichtlichen Bewilligung sagt per se nichts über die Dringlichkeit und das auch über Entführungsfälle hinausgehende Erfordernis einer mündlichen Beauskunftung vorab aus. Die gerichtliche Bewilligung kann im Rahmen des Rufbereitschafts- und Journaldienstes fernmündlich binnen kürzester Zeit erteilt werden, gerade wenn eine unverzügliche Anordnung durch die Staatsanwaltschaft fallspezifisch nötig ist. § 102 Abs. 1 StPO sieht generell vor, dass Anordnungen und Genehmigungen in dringenden Fällen vorläufig mündlich übermittelt werden können. In der Praxis werden solche mündlichen Anordnungen von den Anbietern akzeptiert– wenn eine schriftliche Bestätigung der Exekutive über “mündliche Anordnung und Bewilligung” vorliegt. Auch in diesen Fällen ist Vorkehrung dafür zu treffen, dass eine Beantwortung vor Übermittlung der Anfrage erfolgen kann, wobei gerade hier erforderlich ist, dass die schriftliche Anfrage über die DLS nachzureichen und zu dokumentieren ist.

Zu § 4:

Absatz 1 folgt zunächst dem ersten Grundsatz, den die Richtlinie 2006/24/EG in Art 7 lit a) aufstellt: „Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten“.

Die darüber hinausgehenden Sicherheitsvorschriften, die im 2. Abschnitt geregelt werden und auf die Absatz 2 in diesem Zusammenhang nur verweist, erfließen aus dem Spielraum der Mitgliedsstaaten, höhere Sicherheitsanforderungen zu erlassen (Art 7 Abs. 1 RL 2006/24/EG, arg. „zumindest folgende Grundsätze“) und sind das Ergebnis einer intensiven Diskussion im Rahmen vieler Arbeitsgruppentreffen im Zuge der Umsetzung der Vorratsdatenspeicherung, die nicht zuletzt durch die Entscheidung des deutschen Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010) zur dortigen Aufhebung der deutschen Umsetzung der Vorratsdatenspeicherungs-Richtlinie motiviert und vorgezeichnet sind.

Die für die Ausarbeitung des Konzepts hinter dieser Verordnung wesentlichsten Aussagen des BVerfG sollen hier auszugsweise wiedergegeben werden: Hinsichtlich der Datensicherheit fordert das Gericht „gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben“ (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010, Abs. 225). Dieser hat sich an dem Entwicklungsstand der Fachdiskussion zu orientieren, neue Erkenntnisse und Einsichten fortlaufend aufzunehmen und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten zu stehen. Nur wenn diesbezüglich hinreichende anspruchsvolle und normenklare Regelungen getroffen sind, ist der in einer solchen Speicherung liegende Eingriff verhältnismäßig im engeren Sinne, so das Gericht (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010, Abs. 239). Um in qualifizierter Weise dem Grunde nach den Schutzstandard konkretisieren zu können, muss der Gesetzgeber die Schutzmechanismen selbst benennen und nur deren Ausgestaltung auf Verordnungen oder Aufsichtsbehörden delegieren. Dem ist die Konzeption des § 94

Abs. 4 und 102c TKG 2003 auch gefolgt. Wo die allgemeinen Sicherheitsanforderungen an die Verarbeitung von Telekommunikationsdaten nicht ausreichend sind, um dem speziellen Schutzbedürfnis zu begegnen, das aus der flächendeckenden und anlasslosen Vorratsspeicherung resultiert, werden die besonderen Anforderungen in Ausführung der Vorgaben des § 102c TKG 2003 im nachfolgenden 2. Abschnitt normiert, auf den Absatz 2 klarstellend verweist.

Zu § 5 Abs. 1 bis 4:

Die österreichische Umsetzung ist in einem Punkt weniger streng als das Urteil des deutschen Bundesverfassungsgerichts vorzeichnet, wonach verlangt wird: „Die Daten sind getrennt von den weiteren IT-Systemen des Speicherverpflichteten zu speichern, und zwar hardwaremäßig getrennt und entkoppelt vom Internet." Es genügt also nicht den Anforderungen des Bundesverfassungsgerichts, die Daten, die zur Vorratsdatenspeicherung gedacht sind, durch eine Kennzeichnung in der Datenbank von denjenigen Daten zu trennen, die für Abrechnungszwecke gespeichert werden (Andreas Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399).

Nach den Vorgaben des § 102c TKG 2003 und der Konkretisierung durch § 5 ist eine physische Trennung bei der Speicherung von Vorratsdaten und Betriebsdaten nicht notwendig. Hintergrund dieser Entscheidung des Gesetzgebers und in weiterer Folge des Verordnungsgebers ist die Tatsache, dass eine physische Trennung im Hinblick auf die Datensicherheit nur dann endgültig Sinn ergeben würde, wenn damit auch zwingend verbunden wäre, dass der physische und technische Zugang auf der Ebene der IT-Infrastruktur zu einem solcherart getrennten Speichersystem organisatorisch nur völlig unterschiedlichen Personen im Betrieb des Anbieters möglich ist. Das würde faktisch bedeuten, dass ein zur Speicherung verpflichtetes Unternehmen eine eigene und völlig abgegrenzte IT-Abteilung nur für die Vorratsdatenspeicherung schaffen müsste. Dies wurde in der Debatte zur Umsetzung als unverhältnismäßiger Eingriff in die Eigentumsfreiheit der Anbieter gesehen und hat daher keinen Eingang in die österreichische Umsetzung gefunden. Anzumerken ist, dass sich das deutsche Bundesverfassungsgericht mit dem Problem der flankierenden organisatorischen Trennung gar nicht auseinandergesetzt hat.

Gleichwohl sind die speicherpflichtigen Unternehmen gesetzlich verpflichtet, sicherzustellen, dass der Eingriff auf die Daten einem gesicherten Zugriffsregime unterliegt. Das BVerfG führt hier beispielhaft das Vier-Augen-Prinzip an. Der Zugriff soll nicht durch Einzelne, sondern nur durch zwei oder mehr Personen möglich sein. Darüber hinaus ist der Zugriff auf die Daten revisionssicher zu protokollieren. Damit verlangt das Bundesverfassungsgericht, dass einerseits ein Zugriff auf die Daten nur möglich ist, wenn der Zugriff auch protokolliert wird. Andererseits darf dieses Protokoll nicht im Nachhinein zu verändern sein, muss also revisionssicher sein (siehe dazu die Erläuterungen zu § 7). Um dieses getrennte Zugriffsregime effektiv zu verwirklichen, sind geeignete Maßnahmen sowohl auf technischer als auch organisatorischer Ebene beim Anbieter notwenig, die jedenfalls eine logische Trennung bei der Datenbankhaltung erfordern. Nicht hinreichend wäre dafür, dass die Daten einfach in den betrieblichen Datenbanken verbleiben und dort als Vorratsdaten markiert werden. Daher ordnet Absatz 3 auch an, dass diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen sind. Die konkret von einem Anbieter entwickelte Methode dieser Trennung muss für die Kontrolle durch die Datenschutzkommission nachvollziehbar sein und daher auch dokumentiert werden. Dies sollte der Datenschutzkommission ermöglichen, die tatsächliche Einhaltung der Standards jederzeit zu kontrollieren.

Zu § 5 Abs. 5:

Eine völlige Harmonisierung, wie lange ein Anbieter im Detail welche Daten für betriebliche Zwecke speichern darf, ist kaum zu erreichen und wäre wohl ein unverhältnismäßiger Eingriff in die Erwerbsfreiheit. Die Schwierigkeit liegt nämlich darin, dass die betriebliche Notwendigkeit einer Datenspeicherung einerseits von den technischen Systemen und deren Wartung und andererseits von der Ausgestaltung verschiedener Tarif- und Geschäftsmodelle abhängt. Dabei ist zum Teil gar nicht möglich, dass ein Anbieter in Bezug auf bestimmte Datenkategorien (etwa der Unterscheidung gemäß § 102a Abs. 2 bis 4 TKG 2003 folgend) genau festlegen kann, wie lange diese Datenkategorien jeweils für betriebliche Zwecke aufbewahrt werden. Das Problem liegt nämlich darin, dass zur selben Datenkategorie in unterschiedlichen Tarifmodellen auch unterschiedliche Aufbewahrungszeiträume notwendig sind. Dieselben Daten können also in einem Fall noch Betriebsdaten und in einem anderen Geschäftsmodell bereits Vorratsdaten sein.

Der Anbieter muss jedoch betriebsintern Klarheit darüber schaffen, welche Daten im Hinblick auf die intern bestimmten technischen und geschäftlichen Notwendigkeiten wie lange gespeichert werden. Diese Klarheit ist schon deswegen notwendig, weil ansonsten eine Abgrenzung im Hinblick auf das geforderte

erhöhte Sicherheitsregime bei Vorratsdaten nur schwer möglich ist. Obgleich ein Anbieter Spielraum zur Gestaltung seiner Geschäftsmodelle hat, ist die Unterscheidung von Vorratsdaten nicht völlig beliebig in der Hand des Anbieters. Vielmehr haben die internen Betriebsdaten-Richtlinien den Anforderungen an eine datenschutzrechtliche Rechtfertigung für die Verarbeitung personenbezogener Daten gerecht zu werden. Es muss für einen verständigen Beobachter nachvollziehbar sein, warum bestimmte Daten(Kategorien) für bestimmte Zwecke eine bestimmte Zeit lang aufbewahrt werden. Aus diesem Grund müssen die internen Betriebsdaten-Richtlinien auch der Datenschutzkommission zugänglich sein, damit sie im Falle einer objektiven Kontrolle die Nachvollziehbarkeit der Rechtfertigung prüfen kann.

Überdies muss der Anbieter schließlich in der Lage sein, seine Speicherpolitik gegenüber seinen Kunden zu rechtfertigen, insbesondere für den Fall, dass ein Kunde eine Auskunft gemäß § 26 DSG 2000 begehrt oder im gerichtlichen Verfahren gemäß § 32 DSG 2000 die Richtigstellung oder Löschung seiner Daten begehrt.

Zu § 6 Abs. 1:

Absatz 1 normiert einen für die Praxis wichtigen Größenschluss, dessen Zulässigkeit sich aus den gesetzlichen Voraussetzungen für die Auskunft über Vorratsdaten gemäß § 135 Abs. 2a StPO ergibt. Dieser verweist nämlich auf die Fälle des § 135 Abs. 2 Z 2 bis 4 StPO, woraus sich ergibt, dass immer dann, wenn die Voraussetzungen für eine Auskunft über Vorratsdaten vorliegen, zugleich auch die Vorraussetzungen für eine Auskunft über „Betriebsdaten“ nach § 135 Abs. 2 StPO gegeben sind. Für die Praxis sollen möglichst Fälle vermieden werden, in denen eine Anfrage auf betrieblich gespeicherte Daten negativ beantwortet wird und dann eine zweite Anfrage auf Vorratsdaten erforderlich ist. Es sollen zudem auch Fälle vermieden werden, in denen sich der Zeitraum einer negativen Anfrage auf betriebsnotwendige Daten und die darauf folgenden Anfrage auf Vorratsdaten genau mit jenem Zeitraum überschneidet, innerhalb dessen Daten nicht mehr für betriebsnotwendige Zwecke benötigt werden und somit zu Vorratsdaten werden. Ansonsten könnte es etwa sein, dass Vorratsdaten angefordert werden, zunächst aber nur Betriebsdaten vorliegen und zum Zeitpunkt der nochmaligen Übermittlung des Auskunftsbegehrens gerichtet auf Betriebsdaten (also gemäß § 135 Abs. 2 StPO) diese Daten in der Zwischenzeit doch zu Vorratsdaten geworden sind, und der Anbieter die Antwort schließlich doch auf Basis der ersten Anfrage übermitteln müsste.

Ergänzend erfolgt in Absatz 1 die Klarstellung, dass Protokollierungsverpflichtungen nur dann ausgelöst werden, wenn eine Anfrage über Vorratsdaten erfolgt, die auch einen Zugriff auf (potentiell vorhandene) Vorratsdaten beim Anbieter auslöst, weil es ansonsten in der Statistik auch keine sinnvolle Auswertung zu negativen Beantwortungen geben würde. Wenn beim Anbieter nicht einmal zur Nachschau auf die Vorratsdatenbank zugegriffen wird, etwa weil aufgrund der internen Betriebsdaten-Richtlinie klar ist, dass alle angeforderten Daten noch in den betrieblichen Systemen vorhanden sind, würde ein Protokollierung als Fall der Verwendung von Vorratsdaten nur die Statistik verfälschen. D.h. eine Anfrage nach § 135 Abs. 2a StPO soll nur dann von der Protokollierung erfasst sein, wenn der Anbieter diese nicht allein durch Abfrage der betriebsnotwendigen Daten beantworten kann, sondern tatsächlich gezielt zusätzlich Vorratsdaten abfragen muss. Umgekehrt reicht allerdings schon aus, dass der Anbieter eine Abfrage in der Vorratsdatenbank vornehmen muss, um die Protokollierungspflicht auszulösen, auch wenn diese Abfrage zu keinem Ergebnis führt. Dieser Fall muss in die Statistik als erfolglose Anfrage nach Vorratsdaten Eingang finden.

Zu § 6 Abs. 2:

Aus Sicht der anfrageberechtigten Behörden, Staatsanwaltschaften und Gerichte ist eine Information darüber, ob die abzufragenden Daten betriebsnotwendige Daten oder Vorratsdaten sind, erforderlich. Daher ist hier die Frage relevant, wann einem Datum (besser: einem Datensatz) die rechtliche Qualifikation als „Vorratsdatum“ zukommt. An diese Qualifikation sind nämlich in weiterer Folge erhöhte Konsequenzen im Rechtsschutz geknüpft, beispielsweise die verpflichtende Information der Betroffenen bei Auskünften nach SPG, sowie die besonderen Zugriffs- und Protokollierungsbestimmungen beim Anbieter intern. Für diese Qualifikation findet sich eine Erklärung in den Erläuterungen (GP XXIV, Nr. 1074, 1. Absatz zu § 92 Abs 3 Z 6b TKG 2003): „Bei der Beurteilung, ob es sich bei einem Datum um ein Vorratsdatum handelt, ist vielmehr darauf abzustellen, ob es von Anbietern der in § 102a genannten Dienste ausschließlich aufgrund der Speicherverpflichtung des § 102a gesammelt bzw. gespeichert wird. Dabei ist zu beachten, dass auch beim Anbieter zunächst zu anderen Zwecken vorhandene Daten zu Vorratsdaten werden können, wenn alle anderen zulässigen Speicherzwecke (insbesondere die Betriebsnotwendigkeit der Speicherung) wegfallen. Die Einordnung der Daten als Vorratsdaten ist also durch den Zweck determiniert, zu dem die Daten gespeichert werden (dürfen).“ Nach der Legaldefinition in § 134 Z 2a StPO ist eine Auskunft über Vorratsdaten, „die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach

Maßgabe des § 102a Abs. 2 bis 4 TKG 2003 zu speichern haben, und die nicht nach § 99 Abs. 2 TKG 2003 einer Auskunft nach Z 2 (Anm.: „Auskunft über Daten einer Nachrichtenübermittlung“) unterliegen.“

Für Anfragen, die nicht zwischen Vorratsdaten und betriebsnotwendigen Daten unterscheiden (z.B. nach § 53 Abs. 3a und 3b SPG), muss die Information übermittelt werden, ob Vorratsdaten für die Beantwortung dieser Anfrage verwendet wurden. Umgekehrt kann es sein, dass Anfragen der Staatsanwaltschaft zunächst auf Vorratsdaten gemäß § 135 Abs. 2a StPO gerichtet sind, aufgrund des in Absatz 1 normierten zulässigen Größenschlusses aber tatsächlich keine Vorratsdaten übermittelt werden. In diesen Fällen ist ebenfalls relevant, ob Vorratsdaten verwendet wurden, weil davon die Befassung des Rechtsschutzbeauftragten der Justiz abhängt. Aus diesen Gründen hat der Anbieter bei jeder Übermittlung von Vorratsdaten diesen Umstand als Zusatzinformation (gemäß Anlage, Kapitel 1.4) über die DLS zu übermitteln.

Zu § 6 Abs. 3:

Zu unterscheiden von der rechtlichen Qualifikation als „Vorratsdatum“ ist die Frage nach dem Zeitpunkt der Vorratsspeicherung und der Datenhaltung in der „Vorratsdatenbank“. Hier ist zunächst das Doppelspeicherungsverbot für Vorratsdaten zu beachten. Ein solches ist zwar im normativen Teil der EU-Richtlinie 2006/24/EG nicht ausdrücklich enthalten. Allerdings enthält Erwägungsgrund 13 der RL die Vorgabe: „Die Vorratsspeicherung von Daten sollte so erfolgen, dass vermieden wird, dass Daten mehr als einmal auf Vorrat gespeichert werden.“ Das heißt aber nicht, dass eine gleichzeitige Speicherung von Daten als Betriebsdaten und Vorratsdaten dadurch ausgeschlossen ist. Eine gleichzeitige Speicherung von Daten sowohl in der Vorratsdatenbank als auch in den betrieblichen Datenbanken der Anbieter kann die operative Abwicklung für die Anbieter erleichtern. Die Anbieter könnten nämlich alle Daten schon bei der ersten Verarbeitung aus dem Live-System „abgreifen“ und in die Vorratsdatenbank überführen. Aus den betrieblichen Datenbanken müssen die Daten dann gelöscht werden, sobald die betriebliche Notwendigkeit nicht mehr gegeben ist.

Dazu normiert § 92 Abs. 3 Z 6b des TKG 2003: "Vorratsdaten sind Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden." Für die Beurteilung der Rechtmäßigkeit der in Absatz 3 vorgeschlagenen (nicht verpflichtenden) Zulässigkeit zur gleichzeitigen Speicherung von Betriebsdaten in der Vorratsdatenbank geht es dabei vor allem um die Auslegung des Begriffes "ausschließlich", der aus der Perspektive der Vorratsdatenbank zu verstehen ist. Daten in dieser Datenbank dienen allein dem in § 102a Abs 1 TKG 2003 normierten (und eingeschränkt von § 99 Abs. 5 TKG 2003 mit Ausnahmen durchbrochenen) Zweck der „Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt.“ Zugriffe auf diese Datenbank sind stets nur unter den strengeren Voraussetzungen der §§ 102b und 102c TKG 2003 zulässig, selbst wenn diese Daten zugleich im betrieblichen System des Anbieters vorhanden sind. Insofern wären die Daten in dieser Datenbank – auch bei gleichzeitiger Speicherung in den betrieblichen Systemen des Anbieters – tatsächlich „ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a“ gespeichert. Diese Datenbank würde ab dem Ende der Kommunikation stets alle Daten enthalten, die für Auskünfte gegenüber den berechtigten Behörden, Staatsanwaltschaften und Gerichten zur Verfügung stehen müssen. Dies geht konform mit der Formulierung in § 102a Abs. 1 TKG 2003, derzufolge „nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern“ sind.

Außerdem findet sich in den Erläuterungen zur Regierungsvorlage dazu (GP XXIV, Nr. 1074, 2. Absatz zu § 92 Abs. 3 Z 6b TKG 2003): „Der Begriff „Vorratsdaten“ verdeutlicht explizit, dass die Speicherung der Daten für die in § 102a Abs. 1 festgelegte Dauer ab ihrer Entstehung deshalb flächendeckend und vorrätig erfolgt, damit sie später den Strafverfolgungsbehörden zur Verfügung stehen, falls die Auskunft zu bestimmten Daten einer Nachrichtenübermittlung in einem bestimmten Verfahren zur Ermittlung, Feststellung und Verfolgung einer bestimmten Straftat, deren Schwere eine Auskunft nach § 135 Abs. 2a rechtfertigt, notwendig ist.“

Festzuhalten ist, dass die Zulässigkeit einer sofortigen Speicherung in der Vorratsdatenbank keine Nachteile im Hinblick auf das Schutzniveau nach sich zieht. Vielmehr hätte es Vorteile aus der Sicht des Rechtsschutzes, wenn Auskunftsbegehren beim Anbieter grundsätzlich unter Zugriff auf die Vorratsdatenbank abgewickelt würden, weil dort (im Gegensatz zu den betrieblichen Systemen) ein Zugriff stets nur nach dem Vier-Augen-Prinzip unter revisionssicherer Protokollierung erfolgen darf – auch wenn die Daten zugleich noch in den betrieblichen Systemen des Anbieters vorhanden sein sollten.

Falls Daten, die also auch in den betrieblichen Systemen des Anbieters noch vorhanden sind, beauskunftet werden, muss dies für die Richtigkeit der Statistik sowie allfällige prozedurale Folgen (Informationspflicht nach SPG) in der Vorratsdatenbank jeweils markiert sein. Auskunftsbeantwortungen

könnten dann immer einheitlich über den (protokollierten) Zugriff auf diese Datenbank abgewickelt werden. Der Anbieter muss dann aber jedenfalls in der Vorratsdatenbank über ein „Flag“ pro Datensatz (unterschieden nach den Datenkategorien des § 102a Abs 2 bis 4 TKG 2003) markieren, ob das Datum zugleich noch im betrieblichen System vorhanden ist oder nicht. Bei der Löschung im betrieblichen System müsste dieses „Flag“ dann den Status ändern. Diese Information in der Datenbank (zB: Vorratsdatum J/N) muss dann auch bei der Übermittlung der Antwort zu einem Auskunftsbegehren für die Statistik und zur Kenntnis der Behörden Staatsanwaltschaften und Gerichten mitgeliefert werden (siehe Absatz 2). Sollte ein Auskunftsbegehren nur die Übermittlung von betriebsnotwendigen Daten, nicht aber die Übermittlung von Vorratsdaten erlauben, wäre die Auskunft aus der Vorratsdatenbank nur zulässig, wenn markiert ist, dass die Daten auch in den betrieblichen Systemen noch vorhanden sind.

Zu bemerken ist, dass die durch Absatz 3 eröffnete Möglichkeit in der Praxis nicht von allzu großer Bedeutung sein wird. Die ursprüngliche Intention dieser Möglichkeit aus den Diskussionen zur Umsetzung lag nämlich in der Absicherung, dass Anfragen auf Vorratsdaten auf jeden Fall (wenn überhaupt Daten vorhanden sind) erfolgreich sind, auch wenn dafür Betriebsdaten ausgewertet werden müssen. Dies wird aber nun durch die Normierung des Größenschlusses in Absatz 1 grundsätzlich klargestellt. Die Bedeutung kann aber für kleinere Anbieter bestehen bleiben, wenn gerade mit wenigen Mitarbeitern ein einheitliches Konzept für die Abwicklung von Auskünften gestaltet wird. Große Anbieter werden dies in der Praxis wohl nicht in Erwägung ziehen, weil sich ja auch der benötigte Speicherplatz im Hinblick auf noch betrieblich vorhandene Daten verdoppelt. Vielmehr wird die Abfragelogik (unter Vermeidung von Doppelspeicherung) sowohl Betriebsdaten als auch die Vorratsdatenbank abfragen – letzteres allerdings nur, wenn potentiell Daten in der Vorratsdatenbank vorhanden sein könnten.

Zu § 7 Abs. 1 und 2:

Absatz 1 und 2 dieser Bestimmung sind unmittelbar unter dem Eindruck des Urteils des deutschen Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 Urteil vom 2. März 2010) entstanden. Dort wird ausgeführt: „Wenn der Gesetzgeber eine flächendeckende Speicherung der Telekommunikationsverkehrsdaten ausnahmslos vorschreibt, gehört es zu den erforderlichen Voraussetzungen, dass die betroffenen Anbieter nicht nur ihre Pflicht zur Speicherung, sondern auch die korrespondierenden Anforderungen zur Datensicherheit erfüllen können. Anknüpfend an die sachverständigen Stellungnahmen liegt es nahe, dass nach dem gegenwärtigen Stand der Diskussion grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter der Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt sein müssen, um die Sicherheit der Daten verfassungsrechtlich hinreichend zu gewährleisten (1 BvR 256/08, Absatz 224). Erforderlich sind gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Dabei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Der Gesetzgeber hat dabei jedoch sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt. Die zu stellenden Anforderungen sind entweder durch differenzierte technische Vorschriften – möglicherweise gestuft auf verschiedenen Normebenen – oder in allgemein-genereller Weise vorzugeben und dann in transparenter Weise durch verbindliche Einzelentscheidung der Aufsichtsbehörden gegenüber den einzelnen Unternehmen zu konkretisieren. Verfassungsrechtlich geboten sind weiterhin eine für die Öffentlichkeit transparente Kontrolle (…) sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst (1 BvR 256/08, Absatz 225).“

Diesen Anforderungen wird die österreichische Umsetzung gerecht, indem sie in § 102c TKG 2003 die Notwendigkeit der Unterscheidung von Vorratsdaten und Betriebsdaten, des Vier-Augen-Prinzips beim Zugriff sowie die revisionssichere Protokollierung solcher Zugriffe schon im Gesetz normiert, während die genaueren technischen Vorgaben mit dieser Verordnung geregelt werden. Auch was die Kontrolle durch die Datenschutzkommission betrifft, wird diese abgestufte Regelungstechnik den Anforderungen gerecht. Die für die Öffentlichkeit transparente Kontrolle wird insbesondere dadurch hergestellt, dass die statistischen Daten aus der Protokollierung über die DLS (siehe § 22) gemäß § 102c Abs. 4 TKG 2003 auch dem Nationalrat und dem Datenschutzrat zugänglich sein müssen. Was das ausgeglichene Sanktionensystem betrifft, so greifen hier die bereits bestehenden ausdifferenzierten Haftungsvorschriften des DSG 2000, insbesondere durch § 1 Abs. 5, der im Verfassungsrang die Drittwirkung des Grundrechts normiert und den Rechtsweg an die Zivilgerichte eröffnet. Das Ziel des Vier-Augen Prinzips ist, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Der Zugriff muss dabei nicht durch zwei autorisierte Mitarbeiter des Unternehmens gleichzeitig erfolgen, die

Autorisierung durch die zweite Person kann auch nachträglich erfolgen. „Zeitnah zum Zugriff durch die erste Person“ gibt dabei keine absolute Zeitschranke vor, diese Formulierung indiziert vielmehr, dass zwischen dem Zugriff und der Autorisierung des Zugriffs durch eine zweite Person nicht mehr Zeit vergeht, als im Sinne der arbeitsökonomischen Ausgestaltung der betrieblichen Abläufe noch zumutbar erscheint. Die Anbieter sind zwar nicht verpflichtet, einen „Journaldienst“ zur Beantwortung von Auskunftsersuchen einzurichten, dennoch bieten in der Praxis einige (vor allem große) Anbieter die Möglichkeit, dass Anfragen außerhalb der Geschäftszeiten vor allem durch technisches Wartungspersonal rasch abgewickelt werden, wobei hier regelmäßig nur eine nachträgliche zweite Autorisierung erfolgen kann. Insgesamt muss aber jedenfalls systematisch sichergestellt sein, dass der Anbieter intern über ein effektives Kontrollsystem zur Sicherstellung der Verantwortung verfügt. Dies kann etwa dadurch erreicht werden, dass der Anbieter in kurzen Abständen eine regelmäßige Überprüfung von Zugriffen ohne zweite Autorisierung auch durch technische Ausgestaltung (zB automatische Notifikation) institutionalisiert. Die unmittelbare verfassungsrechtliche Pflicht der Provider aufgrund der Drittwirkung des § 1 Abs. 5 DSG 2000 gebietet auch eine entsprechende Dokumentation schon durch die Anbieter selbst, und nicht nur durch die Strafverfolgungsbehörden, denen die Daten im Auskunftsfall übermittelt werden.

Der Begriff der Revisionssicherheit orientiert sich dabei an den Grundsätzen einer ordnungsgemäßen Buchführung in den unternehmensrechtlichen Vorschriften (insbesondere dem UGB) und dient dem Ziel, die Nutzung nur durch Berechtigte und die Einhaltung der Verfahrensvorschriften sicherzustellen. Die Einhaltung der in Absatz 2 normierten Kriterien ist dabei durch die technische Ausgestaltung des Zugriffsregimes auf die Datenbank sicherzustellen.

Zu § 7 Abs. 3:

Der Inhalt der Protokollierung ist bereits durch § 102c Abs. 2 TKG 2003 detailliert vorgegeben und wird in dieser Verordnung einerseits zur Rechtsklarheit wiederholt, andererseits im Sinne der Eindeutigkeit der zu protokollierenden Informationen um Verweise auf Bestimmungen innerhalb der Verordnung im Zusammenhang mit der Durchlaufstelle ergänzt. Ergänzungen sind insbesondere im Hinblick auf die Erfassung von Speicherzeiträumen bzw. des Datums notwendig. So soll das Datum der Anfrage gemäß Z 3 sich auf die jeweilige Hinterlegung in der Durchlaufstellte beziehen. Diese Daten sind für den Anbieter überdies nur sehr schwer automatisiert zu erfassen (bzw. zu verpacken, da z.B. die Zustellung in das Postfach der DLS nach Erstellung des Protokollfiles beim Anbieter geschieht). Daher wird hierzu in § 23 normiert, dass diese Informationen über die DLS direkt protokolliert und an den Anbieter weitergeleitet werden. Der Anbieter kann sodann diese Protokollinformationen von der DLS für seine interne Protokollierung automatisiert weiterverwenden.

Zu Z 4 wird konkretisiert, dass das Datum zur Aufschlüsselung der abgefragten Datensätze sich auf den Beginn des Kommunikationsvorgangs bezieht, zumal dieser Wert auch im Rahmen der Vorratsdaten gemäß § 102a Abs. 2 bis 4 TKG 2003 relevant ist. Die Ergänzung zu Z 5 basiert auf dem Umstand, dass dem Anbieter nur das Datum der Anordnung gemäß § 138 Abs. 3 StPO (sog. Anbieterausfertigung) bzw. das Datum der Anordnung nach § 53 Abs. 3a oder 3b SPG bekannt ist. Für die Berechnung der Speicherdauer muss der Zeitpunkt der Anordnung der Auskunft mit dem Zeitpunkt der Speicherung als Vorratsdatensatz bzw als Betriebsdatensatz verglichen werden. Da die Anordnung nur ein Datum aber keinen genauen Zeitpunkt enthält, ist für die Berechnung auch nur das Datum der Speicherung als Vorratsdatum relevant, weshalb in Z 5 im Gegensatz zu § 102c Abs. 2 Z 5 TKG 2003 nur das Datum und nicht der Zeitpunkt genannt ist, um Klarheit für die Protokollierung zu schaffen.

Durch Z 8 soll ermöglicht werden, der Forderung von Art 10 der RL 2006/24/EG nachzukommen und auch statistische Daten über die Fälle in welchen Vorratsdaten beauskunftet werden, zu erheben. Die Angabe des zugrundeliegenden Straftatbestands soll bereits beim Auskunftsbegehren auf Seiten der Behörde bzw. der Staatsanwaltschaft oder des Gerichts eingetragen werden. Ein entsprechendes Eingabefeld dafür ist in § 19 vorgesehen, das automatische Abgreifen dieser Information über die DLS für die Statistik ist in § 23 Abs. 2 geregelt.

Zu § 8 Abs. 1:

Siehe die Ausführung zur grundsätzlichen Einigung über das System der DLS und insbesondere die Feststellungen aus dem FIT-Ausschuss bei den Erläuterungen zu § 1.

Zu § 8 Abs. 2 und 3:

Die Vorgaben zur sicheren Übertragung der Daten im Schutzbereich des Telekommunikationsgeheimnisses macht § 94 Abs. 4 TKG 2003: „Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender

und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln." Die Erläuternden Bemerkungen zu § 94 Abs. 4 TKG 2003 (1074 der Beilagen XXIV. GP) führen dazu aus: „Der Spielraum für eine nach dieser Bestimmung zu erlassenden Verordnung ist eng determiniert. Die technische Richtlinie soll für alle Anbieter einheitlich definieren, welche der zu beauskunftenden Werte an welcher Stelle innerhalb der CSV-Datei zu stehen haben und welche Zeichensätze dabei zu verwenden sind. Klar festgelegt ist auch, dass eine Übermittlung der Daten unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie zu erfolgen hat. Zur weiteren Verbesserung des Sicherheitsstandards kann eine asymmetrische Verschlüsselung vorgeschrieben werden. Hier sind allenfalls die näheren technischen Details zur Public Key Infrastructure zu definieren."

Unter einer anspruchsvollen Verschlüsselung ist eine Verschlüsselung zu verstehen, die nach dem derzeitigen Stand der Technik ohne erheblichen Aufwand nicht zu überwinden ist. Dabei ist durch weitere organisatorische Maßnahmen sicherzustellen, dass die Schlüssel und gegebenenfalls das Passwort ebenfalls sicher aufbewahrt werden. Absatz 2 ordnet daher ausdrücklich eine asymmetrische Verschlüsselung an. Bei einem asymmetrischen Verschlüsselungsverfahren besitzt jede der kommunizierenden Parteien ein Schlüsselpaar, das aus einem geheimen Teil (private key) und einem nicht geheimen Teil (public key) besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln. Die kommunizierenden Parteien müssen keinen gemeinsamen geheimen Schlüssel kennen, das Verfahren wird daher auch als Public-Key-Verfahren bezeichnet. Dafür ist eine Public-Key-Infrastruktur erforderlich, über die (vereinfacht dargestellt) die Ausstellung vertrauenswürdiger digitaler Zertifikate zur sicheren Übertragung organisiert wird. Die zentrale Herausforderung liegt darin, sicherzustellen, dass der öffentliche Schlüssel wirklich echt ist. Der Vorteil ist eine deutliche Minimierung des Sicherheitsrisikos, da jeder Benutzer nur seinen eigenen privaten Schlüssel geheim halten muss. Im Gegensatz dazu muss bei einem symmetrischen Verschlüsselungssystem jeder Teilnehmer alle Schlüssel geheim halten, was mit steigendem Aufwand verbunden ist, je mehr Teilnehmer daran beteiligt sind (große Zahl an Schlüsseln). Nachteilig ist, dass asymmetrische Kryptosysteme aufgrund der Verschlüsselungsalgorithmen im Vergleich zu den symmetrischen Verfahren eher langsam sind.

Hybride Verschlüsselungssysteme: Der Geschwindigkeitsnachteil asymmetrischer Verfahren wird in der Praxis durch die Verwendung hybrider Systeme umgangen. Dabei werden die zu übertragenden Daten mit einem zufällig generierten Schlüssel (sog. „session key") symmetrisch verschlüsselt (deutlich schneller) und der jeweils verwendete Schlüssel unter Verwendung einer asymmetrischen Verschlüsselung an die Teilnehmer verteilt. Diese Variante löst das Schlüsselverteilungsproblem und erhält dabei den Geschwindigkeitsvorteil der symmetrischen Verschlüsselung. Das Verfahren entspricht dem Stand der Technik und wird der Anforderung einer technisch anspruchsvollen Verschlüsselung jedenfalls gerecht. Es bleibt jedoch der technischen Spezifikation zur DLS vorbehalten, wie das asymmetrische Verschlüsselungsverfahren der Inhaltsverschlüsselung ausgestaltet wird.

Zu § 8 Abs. 4:

Eine wesentliche Forderung zur Datensicherheit sind die Identifikation und die Authentifizierung des jeweiligen Partners. Das Signaturgesetz kennt dazu die Funktionalität der qualifizierten Signatur, die eine Personenbindung enthält, und der fortgeschrittenen Signatur, die für Unternehmen besser geeignet ist. Das Bundesministerium für Inneres hat die fortgeschrittene Signatur im Portalverbund implementiert und verwendet diese zur Identifikation von Organisationen. Die fortgeschrittene Signatur sollte durch die begleitenden Sicherheitskriterien im Rahmen des Portalverbunds datenschutzrechtlichen Standards genügen. Generell ist es sinnvoll, den Portalverbund, das ist eine Kommunikationsplattform für Bundesdienststellen, auch für die Übermittlung von Anfragen zur Vorratsdatenspeicherung einzusetzen. Die Vorteile der DLS mit Eingliederung in den Portalverbund im Hinblick auf sichere Identifikation, Authentifizierung sowie der sicheren verschlüsselten Übermittlung von personenbezogenen Daten waren in der Diskussion von Beginn an unbestritten. Näheres dazu siehe in den Erläuterungen zu § 13.

Zu § 9:

Am 7.4.2011 wurde die TKG Novelle zur Umsetzung der Vorratsdatenspeicherung im FIT Ausschuss des Nationalrats diskutiert (siehe dazu den Ausschussbericht: 1157 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV. GP). In diesem Rahmen wurde von Ausschussfeststellung beschlossen, in der die grundsätzlichen Annahmen zur DLS wie folgt beschrieben werden: „Für die Datensicherheit und die Nachvollziehbarkeit der Zugriffe auf den Datenvorrat ist das Zusammenspiel der Bestimmungen der §§ 94 Abs. 4 und 102c TKG 2003 von besonderer Bedeutung. Während § 94 Abs. 4 den Aspekt der technischen Datenintegrität und der Determinierung der Verordnungsermächtigung über

die Art der Verschlüsselung betrifft und die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten identifiziert, um durch sichere ‚Identifikation und Authentifizierung von Sender und Empfänger' sicherzustellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden, Staatsanwaltschaften und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht, regelt § 102c Zugriffs- und Sicherheitsbestimmungen. Einerseits muss jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein, um zu gewährleisten, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Andererseits müssen Zugriffe auf Vorratsdaten beim Anbieter revisionssicher protokolliert werden. Die wichtigsten Kriterien sind dabei der Schutz vor Veränderung und Verfälschung, die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens, wozu etwa bei Anordnungen der Staatsanwaltschaft auch die Angabe der Geschäftszahl der ermittelnden Kriminalpolizei zählt. Der Ausschuss geht davon aus, dass sämtliche Zugriffe und Übermittlungen von wem auch immer auf Vorratsdaten gemäß § 94 Abs. 4 TKG 2003 lückenlos protokolliert werden. Der Ausschuss geht weiters davon aus, dass ein automatisches zentrales System der Protokollierung solcher Abfragen und Übermittlungen notwendig ist, wobei unter dieser Protokollierung nicht die in § 102c Abs. 2 genannte zu verstehen ist. Sie wird vielmehr nur jene Daten umfassen, die zur statistischen Auswertung und zur Verknüpfung mit der gemäß § 102c Abs. 2 erfolgenden Protokollierung dient. Wünschenswert ist die Einrichtung einer ‚Datendrehscheibe' (‚Durchlaufstelle', kurz: DLS). Da jeder Auskunftsfall über die DLS mit einer fortlaufenden einmaligen Nummer versehen wird, kann im Falle einer nachprüfenden Kontrolle über die Protokollierung bei der DLS zur Protokollierung beim Anbieter gemäß § 102c Abs. 2 verknüpft werden. Zugang zu den übermittelten personenbezogenen Daten soll die DLS selbst nicht bieten, die Daten liegen dort nur verschlüsselt bis zur Abholung bereit und werden bei der Abholung automatisch gelöscht."

Die Abwicklung der Anfragen und Auskünfte soll über die DLS erleichtert werden, insbesondere die Einbindung über den Portalverbund bringt Synergie-Effekte, weil damit auf Seiten des BMI bereits gute Erfahrungen bestehen. Die DLS ist zugleich die ökonomischste Art der Umsetzung, weil eine sichere Anbindung unter Transport- und Inhaltsverschlüsselung zwischen voraussichtlich 15 anfrageberechtigten Behörden und ca. 200 speicher- und auskunftspflichtigen Anbietern (nach aktuellen Angaben der RTR) über eine zentrale Lösung beim Datenaustausch wesentlich einfacher zu garantieren ist als bei einer dezentralen Kommunikation, zB per E-Mail. Mit der zentralen Lösung der DLS werden sowohl das Fehler- als auch das Sicherheitsrisiko minimiert.

Zu § 10:

Dass das BMVIT die Verantwortung für den Betrieb der Durchlaufstelle übernimmt, ist die sauberste Lösung für die datenschutzrechtlichen Problemstellungen, die mit der zentralen Abwicklung aller Datenauskünfte nach § 94 Abs. 4 TKG 2003 verbunden sind. Der Vorschlag, den Betrieb der DLS und die Beauftragung zur technischen Spezifikation und Umsetzung durch das BMVIT durchzuführen, hat den Grund, dass damit die Bedarfsträger vom Auftraggeber getrennt werden. Weil dem BMVIT keine Aufgaben obliegen, für die eine Verarbeitung von Vorratsdaten notwendig wäre, ist es eine neutrale Stelle ohne eigenes Interesse an den zu übermittelnden Inhalten. Das Interesse des BMVIT am Betrieb der DLS ist darin zu sehen, dass diesem Bundesministerium obliegt, über die Einhaltung der Bestimmungen des TKG 2003 zu wachen, wozu insbesondere auch das Kommunikationsgeheimnis des § 93 TKG 2003 zählt.

Durch die Eigenschaft als Auftraggeber der DLS wird das BMVIT jedoch nicht zum datenschutzrechtlichen Auftraggeber im Hinblick auf die übermittelten Daten. Einerseits besteht nämlich die „Dienstleistung" der DLS nur darin, allen Beteiligten Postfächern für den Datenaustausch zu bieten und bestimmte Aufgaben zur sicheren Übertragung der Daten zu übernehmen. Darüber hinaus müssen die Daten auf eine Weise verschlüsselt werden, dass die DLS gar keine Möglichkeit hat, die Inhalte einzusehen. Die Protokollierung der DLS beinhaltet rein statistische Werte ohne Personenbezug. Die fortlaufende einmalige Nummer jedes Auskunftsvorgang („Unique ID") kann lediglich eine nachprüfende Kontrolle (zB durch Datenschutzkommission, Rechtsschutzbeauftragten oder Gericht) erleichtern, der Personenbezug kann aber über die DLS selbst nicht hergestellt werden.

Nur in einer einzigen Hinsicht ist das BMVIT als datenschutzrechtlich verantwortlicher Auftraggeber zu sehen, nämlich in Bezug auf die Verarbeitung der Information, welche Benutzer überhaupt Auskunftsbegehren über die DLS abwickeln. Ansonsten sind alle personenbezogenen Informationen in der DLS nur verschlüsselt vorhanden, damit sind sie aus der Perspektive der DLS nur indirekt personenbezogen.

Das Bundesrechenzentrum ist überhaupt funktionell Dienstleister im Sinne des § 4 Z 5 DSG, dies jeweils für den Auftraggeber, für dessen Anwendung Daten an die DLS übergeben oder von der DLS übernommen werden. Das heißt, wenn die DLS beispielsweise eine Anordnung der Staatsanwaltschaft in das Postfach des Anbieters zustellt, geschieht dies im Dienst der Behörde, Staatsanwaltschaft oder des Gerichts, von welcher/m die Anordnung stammt. Die Stellung eines datenschutzrechtlichen Auftraggebers kommt dem Bundesrechenzentrum im Hinblick auf den Betrieb der DLS in keiner Phase zu.

Zu § 11:

Die Auditierung betrifft nur die Datensicherheit bei der Durchlaufstelle, nicht aber die Anbieterimplementierungen. Siehe ansonsten die Erläuterungen zu § 18.

Zu § 12:

Die DLS ist ein Modell für technische und prozedurale Abläufe, nicht jedoch eine Art neue Behörde oder Dienststelle. Hierfür muss sich in einer sicheren öffentlichen Infrastruktur (wie jener des Bundesrechenzentrum) ein Server befinden, über den - technisch gesehen - die Anfragen abgewickelt werden. Eine Kommunikation über diesen Server ist dabei nur möglich, wenn die entsprechenden Stellen über eine Berechtigung (Authentifizierung) verfügen.

Für die Ausführung der Mailbox-Funktion der DLS kann es vorteilhaft sein, Webapplikationen und Webservices technisch zu kombinieren, da ein Webservice von der Clientseite flexibel angesprochen werden könnte und somit ein höheres Maß an Benutzerkomfort durch Ausgestaltung des Clients auf der jeweiligen Teilnehmerseite (Behörden oder Anbieter) gestaltbar wäre.

Zu § 13:

Die Unique-ID erfüllt die zentrale Funktion, zusammengehörige Transaktionen zu korrelieren, wobei jede spezifische Behördenanfrage an einen bestimmten Anbieter eine Transaktion darstellt. Beispiel: Eine Anfrage ergeht an zwei Anbieter. Die Unique-ID könnte aus einem einmaligen „Anfrageteil“ sowie einer Anbieter-ID bestehen (1234567-1, 1234567-2); alternativ müsste es eine eigene ID zu dieser Anfrage für jeden Anbieter geben (1234567, 1234568). Die konkrete Ausgestaltung ist in der technischen Spezifikation zur DLS zu klären.

Von Seiten des BMJ wurde in der Diskussion die Anforderung formuliert, dass lückenlos nachvollziehbar sein muss, welche Personen von Anfang bis Ende an einem Auskunftsvorgang beteiligt waren, um allfälligem Missbrauch effektiv begegnen zu können. Die sichere Anbindung der Behördenseite über den Portalverbund bietet sich dabei an, weil hierzu beim Bundesrechenzentrum bereits die vollständige Infrastruktur und ein reicher Erfahrungsschatz besteht. Für die Seite der Anbieter ist ein Portal zu schaffen, dass dem Portalverbund der Behörden nachgebildet ist und denselben Sicherheitsanforderungen entspricht. Auch hierzu besteht beim bereits ein großer Erfahrungsschatz, etwa aus der Realisierung des Elektronischen Rechtsverkehrs (ERV) für die Kommunikation zwischen Gerichten und professionellen Parteienvertretern (Rechtsanwälte, Notare).

Das Prozedere der internen Authentifizierung zur Sicherstellung der konkreten Berechtigung der handelnden Personen muss klar geordnet sein, kann aber im Konzept des Portalverbunds auch intern bei der jeweiligen Organisation (Behörden- oder Anbieterseite) erfolgen und muss nicht zwingend über die DLS technisch realisiert werden, sofern die Anforderungen der Sicherheitsklasse 3 des Portalverbunds erreicht werden; Im Detail vgl. "Spezifikation Sicherheitklassen für den Zugriff von Benutzern auf Anwendungen", Version 2.1.0, 8.2.2008, ["SecClass 2.1.0"; Anhang zur Portalverbundvereinbarung pvv 1.0, 21.11.2002]. Es sind die Konventionen des Portalverbunds einzuhalten, wobei die Bundesrechenzentrum GmbH Teilnehmer am Portalverbund ist. Die Stammportale werden von den einzelnen Institutionen betrieben (oder von deren Dienstleistern).

Der Portalverbund Österreich ist eine E-Government Anwendung und wird auf der Website „Digitales Österreich“ (http://www.digitales.oesterreich.gv.at/site/5288/default.aspx) wie folgt beschrieben: „Der Portalverbund ist ein Zusammenschluss von Verwaltungsportalen zur gemeinsamen Nutzung von bestehender Infrastruktur. Grundsätzlich haben Portale den Vorteil, dass mehrere Applikationen über einen Punkt zugänglich werden. Die Identität der Benutzenden wird im Zuge des Anmeldevorganges am Portal nur einmal überprüft. Die Benutzenden müssen sich daher nur einmal "ausweisen" um auf mehrere Ressourcen zugreifen zu können. Betreibenden von Anwendungen wird es im Portalverbund ermöglicht, die Authentifizierung und Autorisierung zu Portalen in Vertrauensstellung auszulagern. Anstelle einer eigenen Benutzerverwaltung für jede Anwendung wird nur mehr eine Benutzerverwaltung am Stammportal benötigt. Dadurch wird die Benutzerverwaltung vereinfacht und ein Single Sign-On unterstützt. Die Benutzerverwaltung bleibt technisch und organisatorisch weiterhin im Verantwortungsbereich der personalführenden Stelle. Organisationen, die am Portalverbund teilnehmen,

können ihre lokale Benutzerverwaltung nicht nur für interne Anwendungen, sondern auch für externe Applikationen und Anwendungen verwenden. Betreiber von Applikationsportalen bleibt somit die externe Benutzerverwaltung erspart.

Die Teilnahme am Portalverbund wird durch die Portalverbundvereinbarung geregelt. Diese enthält Rechte und Pflichten, die von den teilnehmenden Portalbetreibenden einzuhalten sind. Zwischen den Betreibenden von Stammportalen, welche die Benutzenden verwalten und Anwendungsbetreibenden wird so ein Vertrauensverhältnis hergestellt. Alle Vereinbarungen werden bei einem Depositar, das ist jenes Bundesministerium, das für die IT-Koordination des Bundes zuständig ist, aufbewahrt. Technisch und organisatorisch ist die Kommunikation im Portalverbund durch das Portalverbundprotokoll (PVP) und durch die Festlegung von Sicherheitsklassen geregelt. Die Definition von Sicherheitsklassen im Portalverbund ermöglicht es einer Anwendung zu prüfen, ob Benutzende die für die Nutzung der Anwendungsfunktion erforderlichen Sicherheitsauflagen erfüllen. Für Mitarbeitende von Institutionen, die am Portalverbund teilnehmen, ergeben sich keine Veränderungen.

Der Betreibende von Anwendungen bestimmt, welche Anwendungen über welches Anwendungsportal zugänglich sind. Der Betreibende legt unter Beachtung sämtlicher Datenschutzbestimmungen fest, welche Stellen beziehungsweise Kategorien von Stellen über ein Anwendungsportal zugriffsberechtigt sind und definiert für seine Anwendungen je nach Aufgabenstellungen der Benutzenden Rollen mit entsprechenden Rechteprofilen. Der Stammportalbetreibende muss unter anderem sicherstellen, dass über das eigene Portal nur berechtigte Benutzende ordnungsgemäß auf Anwendungen zugreifen. Der Anwendungsportalbetreiber muss sicherstellen, dass nur über ein Stammportal autorisierte Benutzende auf die durch das Portal erreichbaren Datenanwendungen zugreifen können. Die Übereinstimmung des Rechteprofils der Benutzenden mit den Zuständigkeiten der zugriffsberechtigten Stelle muss geprüft werden. Erforderliche Datensicherheitsmaßnahmen sind ebenfalls zu organisieren und umzusetzen. Betreiber von Stammportalen können sich für den technischen Betrieb eines Dienstleistenden bedienen. In diesem Fall ist vom Dienstleistenden eine Vereinbarung zu unterzeichnen, die gewährleistet, dass auch dieser alle technischen und organisatorischen Vorkehrungen einhält, auf denen das Vertrauensverhältnis der Portalverbund-Teilnehmenden beruht.“

Zu § 14:

Die Anzahl der zugangsberechtigen Dienststellen der Sicherheitsbehörden wird durch Erlass der Bundesministerin für Inneres festgelegt jener im Bereich der Justizbehörden wird durch das Bundesministerium für Justiz festgelegt und der Bundesrechenzentrum GmbH für die Spezifikation der Durchlaufstelle bekanntgegeben.

Zu § 15:

Ein wesentlicher Vorteil des Konzepts der DLS ist die Verringerung der Kommunikationswege. In den Diskussionen ging man von 15 anfrageberechtigten Behörden und 200 auskunftspflichtigen Netzen (alle die der Verpflichtung zur Entrichtung des Finanzierungsbeitrages zur RTR unterliegen) aus. Insbesondere kleinere Anbieter haben geringere Ressourcen. Daher ist es die effizienteste Vorgangsweise, nur mit einer Stelle zu kommunizieren. Spezielle technische Voraussetzungen auf Anbieterseite sind keine nötig, da die DLS über eine sichere Verbindung (die wahrscheinlich über das Protokoll „https“ realisiert werden wird) praktisch mit jedem gängigen Browserprogramm erreichbar wäre. In welchem Ausmaß ein Anbieter seine Prozesse bis zur Erstellung des „CSV-Files“ mit den begehrten Daten automatisiert, bleibt ihm selbst überlassen, was insbesondere für kleinere Anbieter wichtig ist, bei denen eine teure Automatisierung in keinem Verhältnis zur Zahl der jährlichen Auskünfte steht.

Zu § 16:

Bei der Anbindung der Anbieter ist sicherzustellen, dass auf Anbieterseite möglichst flexibel auf die DLS zugegriffen werden kann, damit auch außerhalb der Geschäftszeiten eine möglichst rasche Beantwortung des Auskunftsbegehrens erfolgen kann.

Die Sicherheitsstufe 3 aus der “Definition der Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich E-Government” ist abrufbar unter http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=21832 und dort wie folgt beschrieben:

„Die höchste Sicherheitsstufe im Bereich E-Government, die auch für die Kommunikation Verwaltung – Verwaltung angewandt werden kann, wenn dies die Vertraulichkeit erfordert, wurde darauf ausgelegt, dass sie kompromittierten Endgeräten stand hält. Bei Anwendung dieser Sicherheitsstufe haben Client und Server Klarheit darüber, wer kommuniziert und können auch von der Vertraulichkeit im Rahmen der Sicherheit der kryptographischen Schlüssel und Algorithmen ausgehen.

Die Sicherheit wird mit einer TLS-Verbindung erreicht und basiert auf Zertifikaten mit Verwaltungseigenschaft. Die Bindung der Zertifikate an Client und Server ist technisch so abzusichern,

dass sie auch kompromittierten Endsystemen standhält. Die für den Ablauf notwendigen Zertifikate werden direkt vom Server bzw. Client in die sichere TLS-Verbindung eingebunden. Es wird somit, anders als bei Stufe II, eine automatische und in die Verbindungsprotokolle integrierte Überprüfung der Serveridentität möglich. Dieser Mechanismus kann nun auch automatisch man-in-the-middle Attacken erkennen.

Die Zertifikate des Clients und des Serves der TLS-Verbindung werden in vertrauenswürdigen Komponenten gehalten und sind technisch vor Modikation geschützt. Dies kann zum Beispiel durch den Einsatz von hardware security modules (HSM), auch Kryptoboxen genannt, erreicht werden. Diese Sicherheitsmodule sind in verschiedenen Formaten (Box, Tischgerät, PC-Karte, Chipkarte) erhältlich und werden in der Regel als interne Karten, als periphere Geräte oder über einen Adapter (für die Chipkarte) an den Hostrechner (Zentralrechner, Server, PCs) angeschlossen. Eine weitere Möglichkeit zur Absicherung besteht im Schaffen einer vertrauenswürdigen Softwareumgebung, unter anderem mit sicherem boot - Prozess, zuverlässigem Betriebssystem und digital signierter Software. Diese Sicherheitsstufe ist für Transaktionen mit sensiblen Daten nach dem Datenschutzgesetz geeignet (analog Sicherheitsklasse 3 im Portalverbund).“

Zu § 17:

Die in § 17 klar vorgezeichneten Abläufe der Zustellung von Auskunftsbegehren und Antworten in die Postfächer der jeweils Beteiligten sind zentral für die Architektur der DLS und erfüllen auch eine wesentliche datenschutzrechtliche Funktion. Damit ist nämlich auch von der technischen Konzeption her eindeutig, dass die Auskunft über Daten, die vom Schutzbereich des DSG 2000 und des Kommunikationsgeheimnisses des § 93 TKG 2003 erfasst sind, immer in Form eines „push“ aus der Sicht des Anbieters erfolgt. Lediglich die Abholung der Anordnung durch den Anbieter einerseits und die Abholung der Antwort durch die Behörde andererseits kann durch den Einsatz von Webservices teilautomatisiert werden. Dadurch entsteht aber keine vollautomatisierte Schnittstelle mit unmittelbarem Zugriff der Behörden auf die Datenbanken der Anbieter. Die Mediatisierung über die DLS als Postfachsystem stellt eine faktisch effektive Begrenzung der staatlichen Kontrollmacht dar.

Zu § 18:

Die fortgeschrittene Signatur stellt die praktikabelste Lösung dar und beinhaltet die Möglichkeit eines Zertifikats auf Unternehmensbasis. Die Zuordnung zu Einzelpersonen ist in den Protokolldateien ersichtlich und muss daher nicht unbedingt durch die Signatur erfolgen. Durch die Signatur wird auch ein Hashwert zur Wahrung der Datenintegrität überflüssig. Mit der Signatur kann im Gegensatz zum bloßen Hashwert auch die Identität des Signators überprüft werden. Man weiß dann nicht nur, dass die Daten korrekt sind, sondern dass sie auch tatsächlich vom Signator stammen. Bei der Verwendung eines bloßen Hashwerts könnte ein „Man-In-The-Middle“ die Nachricht und den Hash abfangen, beides ändern, und die geänderten Versionen der Nachricht und des Hashwerts weiterschicken. Hashwerte (in diesem Kontext) alleine schützen nur vor zufälligen Veränderungen, Signaturen auch vor absichtlichen Manipulationen.

Für die verschlüsselte Übermittlung von Auskunftsdaten wird der öffentliche Schlüssel (auch: public key) des jeweiligen Empfängers verwendet. Nur dieser kann dann mit seinem private Schlüssel (auch: private key) die Auskunft im Klartext lesen. Die bei der DLS angesiedelte Aufgabe der Schlüsselverwaltung bedeutet, dass die öffentlichen Schlüssel zur Verschlüsselung der Daten am DLS-Server technisch gesehen durch sog. „Zertifikate“ hinterlegt werden. Die Verschlüsselung der Anfrage und der Antwort kann nur bei der Behörde bzw. beim Anbieter stattfinden. Für die Verschlüsselung wird der „private key“ benötigt und dieser kann niemals von der DLS erzeugt oder gespeichert werden. Die DLS ist nur für die Transportverschlüsselung zuständig und kennt natürlich die dafür notwendigen Schlüssel.

Zu § 19:

Im Zuge der Diskussion zum zeitlichen und finanziellen Rahmen der Umsetzung eines Datensicherheitskonzepts wurde die so genannte "Implementierung Light" der Durchlaufstelle diskutiert. Darunter sind jene Änderungen im Konzept zu verstehen, die sich seit der ersten Vorstellung des Konzepts der Durchlaufstelle aus der Diskussion ergeben haben. Dazu gehört einerseits die Implementierung im Rahmen des Portalverbundes. Damit kann die interministerielle Seite und die Anbieterseite der Implementierung getrennt werden. Für die Spezifikation und Implementierung der interministeriellen Seite ist keine Einbindung der Netzbetreiber mehr erforderlich. Die zweite Eigenschaft der "Durchlaufstelle Light" betrifft die Formalisierung der Anfragen. Für Anfragen nach dem SPG ist heute bereits eine Verwendung von normierten Formularen gemäß Erlass des BIM vorgesehen. Bei Anfragen nach der StPO gibt es zwar Formulare, denen jedoch kein zwingender Erlass zugrunde liegt und die in der Praxis auch nicht durchgehend verwendet werden. Anfragen nach der StPO enthalten als Beilage die Anordnung des Staatsanwalts mit der prosaischen Beschreibung des Auskunftsbegehrens.

Mittelfristig wurde in der Diskussion das Ziel formuliert, auch für Datenanfragen nach der StPO eine Formalisierung über Eingabemasken zu erreichen. Es sollte allerdings zugleich verhindert werden, dass Anbieter durch den Vergleich einer allenfalls per Webmaske ausgeführten Anordnung mit dem beiliegenden Original der StA Anordnung einen erhöhten Aufwand haben. Zur Optimierung der Betriebsabläufe ist jedenfalls ein Rückkanal vorzusehen. Das heißt etwa, dass bei Differenzen zwischen den begehrten Daten und der beiliegenden Anordnung der StA eine Antwort an die abfrageberechtigte Stelle zu schicken ist, mit der darauf hingewiesen wird, dass diese Fehler zu korrigieren sind. Zu diesem Zweck regelt die Verordnung in § 20 die Möglichkeit von „Zusatzinformationen“. Für die Implementierung der Durchlaufstelle bedeutet dies, dass in der Phase der ersten Implementierung jedenfalls StPO-Anordnungen übermittelt werden können müssen, ohne dabei an bestimmte online-Formulare über die Webmaske gebunden zu sein.

Zusammengefasst bedeutet das:

Die DLS ist zwingend die Drehscheibe zur Kommunikation für alle Auskunftsfälle. Kern ist dabei, dass die jeweilige Seite ihre Anforderung/Antwort sicher über die DLS samt dem notwendigen Anhang (Anbieter-Anordnung nach § 139 Abs. 3 StPO, CSV-Datei mit den begehrten Daten) übermittelt.

Die Spezifikation der DLS muss jedoch nicht enthalten, wie auf Seiten der Behörden die jeweiligen Web-Formulare aussehen. Eine Formalisierung wird jedoch auf Behördenseite aus eigenem Interesse einer einheitlichen und geordneten Abwicklung angestrebt.

Auch auf der Seite der Anbieter muss nicht spezifiziert werden, ob, inwieweit und wie die Beantwortung von Auskunftsbegehren (teil-)automatisiert wird. Durch die Anlage zu dieser Verordnung wird einheitlich festgelegt, wie die CSV-Datei aussehen muss. Wie die einzelnen Anbieter diese Datei „befüllen“ bleibt deren Entscheidung.

Der Vorschlag enthält lediglich, dass bei der Übermittlung eines Auskunftsbegehrens via DLS ausgewählt werden muss, auf welcher Rechtsgrundlage die Anordnung ergeht. Dies dient der statistischen Erfassung über die DLS und beinhaltet keine Determinierung der Formulare oder Webmasken, die bei den Behörden für die Anordnungen verwendet werden. Eine Determinierung ergibt sich allerdings aus der Spezifikation der Felder der CSV-Datei gemäß dem Vorschlag in der Anlage.

Zu § 20:

Die CSV-Dateien werden mittels sicherem Filetransfer und Inhaltsverschlüsselt an die Durchlaufstelle übermittelt. Zusatzinformationen könnten allenfalls über ein Web-Interface zu der entsprechenden Abfrage eingegeben werden. Diese Zusatzinformationen könnten etwa Gründe für eine Leer-Meldung beschreiben. Ob und in welchem Ausmaß ein Web-Interface auf Seiten der DLS zur Verfügung gestellt werden soll, wird Gegenstand der Diskussion zur Spezifikation der DLS sein. Jedenfalls ist dabei zu bedenken, dass die DLS gegenüber Inhalten der Auskünfte "blind" sein soll, personenbezogene Informationen sollten also nicht als Zusatzinformation übermittelt werden, weil diese gegenüber der DLS nicht inhaltsverschlüsselt werden, sondern nur durch die Transportverschlüsselung vor Zugriffen von außen sicher sind. Alternativ ist auch möglich nach dem sonstigen Aufbau der EP 020 die möglichen Dateiformate und Dateinamen für Zusatzinformationen zu definieren. Auf diese Weise könnten auch personenbezogene Zusatzinformationen mit Inhaltsverschlüsselung übertragen werden, die aus Sicht der DLS nicht zugänglich sind. Für Anfragen, die nicht zwischen Vorratsdaten und betriebsnotwendigen Daten unterscheiden (z.B. nach § 53 Abs. 3a und 3b SPG) muss jedenfalls die Information übermittelt werden, ob Vorratsdaten für die Beantwortung dieser Anfrage verwendet wurden. Diese Information wird von den Anbietern als "Zusatzinformation" übermittelt (siehe § 6 Abs. 2).

Allenfalls könnte für die Übertragung von Zusatzinformationen eine Textdatei (.doc/.txt) zum Einsatz kommen, welches leicht wie eine “reale Antwort” mit dem Schlüssel der Behörde verschlüsselt wird. In diesem Fall hier wäre die Benennung dieser Datei in der Spezifikation zur DLS zu regeln.

Zu § 21:

In den Grundsatzdiskussionen zur DLS wurde die Möglichkeit einer elektronischen Stammdatenauskunft im Bereich der Telefon-Anbieter als optionale Variante besprochen. Festgehalten wird aus dieser Diskussion, dass es aus Sicht des BMI nicht darum geht, eine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters herzustellen. Vielmehr besteht der Wunsch nach einem elektronischen Hin- und Rückkanal, der zu einer möglichst raschen Abwicklung führt. In wie weit ein Anbieter solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-)Automatisierung in eigener Verantwortung die Auskünfte optimieren. Wesentlich ist, dass eine Anbindung an ein elektronisches System für Stammdatenauskünfte über die DLS nicht gesetzlich verpflichtend als ausschließliche

Übermittlungsvariante für alle Anbieter eingerichtet werden muss. Durch die Verordnung soll lediglich die optionale Möglichkeit einer solchen Anbindung normiert werden. Wenn zumindest die großen (insbesondere Mobilfunk-) Anbieter sich anschließen, würde der Zweck erfüllt.

In einer solchen Anfrage würde eine Rufnummer übermittelt. Dazu sind vom Anbieter die zugehörigen Stammdaten für den Anfragezeitraum, längstens aber 6 Monate zurück, zu ergänzen. In der bisherigen Praxis werden vor einer Anordnung zu einer Verkehrsdatenauskunft zunächst zu einer (oder mehreren) bestimmten Nummer Stammdatenauskünfte begehrt, wobei diese Auskunftsbegehren an alle in Frage kommenden Anbieter gerichtet werden (bei Mobilfunk ist die Zahl dabei überschaubar, weil es nicht so viele Anbieter gibt). Aufgrund der Antworten weiß die Behörde dann, für welche Zeiträume bei welchem Anbieter Verkehrsdaten vorhanden sein könnten, und kann das Auskunftsbegehren zielgerichtet stellen. Die Stammdatenauskunft wird in der Praxis auch deshalb regelmäßig vorgelagert, weil die Kriminalpolizei damit bereits einen ersten Filter setzt, welche Teilnehmeranschlüsse ermittlungsrelevant sein könnten. Als Antwort werden Stammdaten, der entsprechende Zeitraum und die Information „aktiv“ oder „inaktiv“ übermittelt. Es können auch bei einem Anbieter zur gleichen Rufnummer während der letzten 6 Monate mehrere Stammdatensätze anfallen (z.B. bei einer Übertragung der Rufnummer).

Die Praxis der vorgelagerten Stammdatenauskünfte wird auch im zukünftigen Auskunftsregime über die DLS weiterhin relevant bleiben. Um solche Stammdatenabfragen zu erleichtern bzw. zu beschleunigen sieht der Entwurf zur Verordnung vor, dass Anbieter im Einvernehmen mit den abfrageberechtigten Behörden für eine Abwicklung von Stammdaten-Auskünften via DLS optieren können. Eine Abwicklung von Stammdatenauskünften über die DLS soll nicht verpflichtend als ausschließliche Übermittlungsvariante für alle Anbieter eingerichtet werden. Außerdem soll keine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters hergestellt werden, diese soll vielmehr über die DLS mediatisiert werden. Es soll lediglich einen elektronischen Hin- und Rückkanal geben, der zu einer möglichst raschen Abwicklung führt. In wie weit ein Anbieter solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-)Automatisierung in eigener Verantwortung die Auskünfte optimieren.

Zu § 22:

Welche Informationen der Anbieter bei der Abwicklung von behördlichen Auskunftsbegehren zu protokollieren hat, ist bereits detailliert in § 102c Abs. 2 TKG 2003 geregelt und wird im Sinne der Rechtsklarheit in § 7 Abs. 3 mit ergänzende Verweisen auf relevante Bestimmungen dieser Verordnung wiederholt. Diese Bestimmung zur Protokollierung bezieht sich indes auf jene Protokoll-Informationen, die der Anbieter gemäß § 102c Abs. 4 TKG 2003 an die dort genannten Stellen (Datenschutzkommission, Datenschutzrat, BMJ) zu übermitteln hat. Bei der Entwicklung des Konzepts der Durchlaufstelle wurde dabei bedacht, dass die zentrale Sammlung der für die Statistik notwendigen Protokollinformationen für diese Zwecke in der DLS eine enorme Verfahrens- und Verwaltungsvereinfachung darstellt. Dabei werden jene – nicht personenbezogenen – Informationen aus der Protokollierung beim Anbieter mit der (verschlüsselten) Auskunft unverschlüsselt mitgeliefert, sodass diese in der DLS für die Aufbereitung der Statistik gespeichert werden können. Diese Methode ist zugleich ein wertvoller Beitrag zur Datensicherheit, weil damit zugleich eine revisionssichere Protokollierung aller Auskunftsfälle in der DLS selbst erfolgt. Für den Fall, dass die Rechtsschutzbeauftragten, die Datenschutzkommission oder ein Gericht im Verfahren gemäß § 32 DSG 2000 für die Überprüfung der Rechtmäßigkeit eines bestimmten Falles der Datenübermittlung die exakten personenbezogenen Daten benötigt, die auf der Seite der Anbieter gemäß § 7 gespeichert werden und auch auf Seiten der Behörden nach den für diese einschlägigen (internen) Verfahrensvorschriften zu erfassen und aufzubewahren sind, kann die statistische Erfassung über die DLS äußerst hilfreich sein. Über die Unique-ID (§ 13) kann nämlich im Rechtsschutzfall der gesamte Ablauf vom Auskunftsbegehren bis zur Beantwortung lückenlos nachvollzogen werden und die richtigen Protokolldaten werden so auf der jeweils überprüften Seite (Anbieter oder Behörden) leichter auffindbar.

Deutlich vereinfacht wird dabei auch das Verfahren für die Aufbereitung der Statistik, die das BMJ jährlich an die EU-Kommission gemäß Art 10 der Richtlinie 2006/24/EG zu übermitteln hat. Über die DLS werden nach dieser Bestimmung alle Rohdaten automatisch gesammelt, die für die Statistik notwendig sind. Die automatische Aufbereitung der Statistik in der DLS richtet sich nach § 23. Hier ist darauf hinzuweisen, dass in der TKG Novelle zur Umsetzung der Vorratsdatenspeicherung ein Redaktionsversehen unterlaufen ist, das dazu führen würde, dass die notwendigen Rohdaten zur Erfüllung dieser gemeinschaftsrechtlichen Verpflichtung unmöglich machen würde. § 102c Abs. 4 Z 2 ordnet nämlich an, dass die Anbieter die Protokolldaten gemäß § 102c Abs. 2 Z 2 bis 4 an das BMJ zu übermitteln haben. Damit würden die Anbieter für die Statistik die Aktenzahlen zu den Auskunftsfällen nach SPG (Z 2 leg cit) übermitteln, nicht aber die Information zur Speicherdauer der übermittelten Daten

(Z 5 leg cit), die nach Art 10 Abs. 1 zweiter Spiegelstrich RL 2006/24/EG ausdrücklich gefordert sind. Dieses Versehen entstand dadurch, dass die Z 2 in § 102c Abs. 2 TKG 2003 im Zuge der Entstehung der Regierungsvorlage erst nachträglich eingefügt wurde, die entsprechende Anpassung im Absatz 4 aber unterblieb. In Absatz 2 dieser Bestimmung erfolgt daher durch den Verweis auf § 7 Abs. 3 Z 3 bis 5 die Korrektur dieses Redaktionsversehens. Um zu vermeiden, dass die Verordnung aus rein formalistischen Gründen wegen Gesetzwidrigkeit beim Verfassungsgerichtshof angefochten und möglicherweise in diesem Punkt für nichtig erklärt wird, sollte der Gesetzgeber daher schnellstmöglich die Richtigstellung im Gesetz selbst vornehmen, um zu vermeiden, dass die europarechtlichen Verpflichtung zur Übermittlung der Statistik aufgrund eines bloßen Versehens nicht erfüllt werden kann.

Zu § 23:

Einerseits müssen die sog. provider-internen Protokolldaten vorliegen (vgl. § 102c Abs 1 TKG 2003). Anbieter müssen intern revisionssicher protokollieren, dass Zugriffe auf Vorratsdaten unter Einhaltung des Vier-Augen-Prinzips nur durch speziell ermächtigte und bestimmte Personen und nur aufgrund einer entsprechenden behördlichen, staatsanwaltschaftlichen bzw. gerichtlichen Anfrage erfolgt sind. Diesen Zugriffen muss immer ein behördlicher, staatsanwaltschaftlicher bzw. gerichtlicher Auftrag zugrunde liegen, insofern besteht ein Zusammenhang zu den Protokoll-Daten über die Auskunftsfälle. Dem gegenüber stehen jene Protokoll bzw Statistik-Aufzeichnung über erfolgte Vorratsdaten-Abfragen (vgl. § 102c Abs 2 TKG 2003), die einmal jährlich an die Europäische Kommission zu übermitteln sind.

Diese beiden Protokollverpflichtungen überschneiden sich allerdings im Hinblick auf den Informationsgehalt. Die Protokollierung für die Statistik muss diese provider-internen Informationen (also welche Mitarbeiter wann zugegriffen haben) allerdings nicht enthalten.“

Es besteht eine Verpflichtung zur jährlichen Berichterstattung gegenüber der Europäischen Kommission, die vom BMJ wahrzunehmen ist. Die Erfassung der Protokolldaten im Rahmen der Durchlaufstelle soll diese Erfassung der Protokolldaten für die Anbieter sowie das BMJ deutlich vereinfachen. Denn ansonsten müssen die Protokolldaten von allen Providern eingesammelt und in einheitlicher Struktur zusammengeführt werden. Die Harmonisierung der Protokoll-Struktur müsste also jedenfalls geregelt werden. Gemäß § 102c Abs. 4 Z 2 TKG 2003 obliegt es weiters auch dem BMJ, dem Nationalrat über die Statistik zu berichten.

Es macht jedenfalls Sinn, die Information zum Zeitpunkt der Zustellung der Anordnung in das Postfach des Anbieters gemäß § 7 Abs. 3 Z 3 schon bei der Anfrage zu protokollieren und damit den Protokoll-Datensatz zu einer Anfrage zu „eröffnen“. Alle Anfragen über die DLS sind mit einer "Unique-ID" versehen. Die vom Anbieter übermittelte Antwort ist über dieselbe "Unique_ID" verknüpft und kann so den Datensatz zur Protokollierung mit den weiteren benötigten Informationen ergänzen. Gleichermaßen wird der Zeitpunkt der Zustellung der Antwort in das Postfach des Anbieters von der DLS selbständig protokolliert.

Zu § 24:

Diese Bestimmung dient der Klarstellung der Kostentragung der Investitionskosten für die Durchlaufstelle. Nähere Ausführungen über die finanziellen Auswirkungen sind im Vorblatt dargestellt.

Die Aufteilung der laufenden Kosten der DLS (Betriebskosten) bleibt einer interministeriellen Vereinbarung vorbehalten.

Zur Anlage (Schnittstellendefinition EP020):

Die Schnittstellendefinition erfolgt aus Gründen der besseren Darstellung in Form einer Anlage. In der Beilage zu den Erläuternden Bemerkungen werden für alle in der Anlage definierten Datenfelder Beispiele dargestellt. Die Aufzählung der Beispiele ist nicht abschließend und soll den Anbietern sowie den auskunftsberechtigten Behörden zur Hilfestellung bei der technischen Implementierung dienen. Entsprechend kommt dieser Beilage keine über die Anlage oder die sonstigen Bestimmungen dieser Verordnung hinausgehende Bedeutung zu.

Aus den EB zur RV (1074 der Beilagen XXIV. GP - Regierungsvorlage - Vorblatt und Erläuterungen): „Der Spielraum für eine nach dieser Bestimmung zu erlassenden Verordnung ist eng determiniert. Die technische Richtlinie soll für alle Anbieter einheitlich definieren, welche der zu beauskunftenden Werte an welcher Stelle innerhalb der CSV-Datei zu stehen haben und welche Zeichensätze dabei zu verwenden sind.“

Die Technische Richtlinie in der Anlage basiert auf einer Empfehlung (EP020), die innerhalb der Telekom-Branche im Rahmen des Arbeitskreis-Telekommunikation (AK-TK) durch die Arbeitsgruppe „Schnittstellendefinition“ bereits während der Entstehung der TKG-Novelle zur Umsetzung der Vorratsdatenspeicherung ausgearbeitet wurde. Die EP020 wurde im Rahmen der insgesamt 6 Round

Table Diskussionen des BIM im Zuge der Studie zur Datensicherheit (im Auftrag des BMVIT) mit allen Beteiligten (insbesondere BMI und Bundeskriminalamt) diskutiert und abgestimmt (siehe dazu ausführlich die EB zu § 1). Die Technische Richtlinie in der Anlage enthält all jene Teile der EP020, die sich unmittelbar auf die Definition der Syntax und Semantik der CSV Datei für die Übermittlung von Auskünften bezieht. Die EP020 als ganzes ist in der Datensicherheitsstudie abgebildet und in diesem Rahmen auch zur Veröffentlichung freigegeben.

Anlage

Technische Richtlinie zur CSV-Datei für die Beantwortung von Auskunftsbegehren gemäß § 94 Abs. 4 TKG 2003 – EP020

1. Syntax und Semantik der CSV-Datei gemäß § 94 Abs. 4 TKG 2003

Diese technische Richtlinie definiert die Syntax und die Semantik der Daten, die einer Behörde im Rahmen einer Beauskunftung übermittelt werden.

1.1 Datenformat

Gemäß § 94 (4) TKG 2003 wird das CSV („Comma-Separated Values“) Format nach IETF RFC 4180 verwendet. Das CSV Format besteht demnach aus Records, die durch Zeilenschaltung getrennt sind. Jeder Record enthält Datenfelder, welche durch Komma (Hexadezimal 2C) getrennt sind. Alle Datenfelder werden durch Anführungszeichen (double quote – Hexadezimal 22) begrenzt. Wenn Anführungszeichen Inhalt eines Datenfeldes sind, wird ein weiteres Anführungszeichen vorgesetzt. Metadaten wie n.a. oder # (siehe Kapitel 1.1.17.) werden nicht unter Anführungszeichen gesetzt. Jeder Record wird durch CRLF (Carriage Return - Hexadezimal 0D, Line Feed - Hexadezimal 0A) abgeschlossen.

Jedes „csv“-File bildet die Auskunft zu einem bestimmten Indikator und einer bestimmten Datenart ab. Die optionalen Parameter des CSV Formats gemäß RFC 4180 und die Kodierung der Datenfelder werden wie folgt festgelegt:

1.1.1 Zeichensatz

Als Zeichensatz wird UTF-8 (RFC 3629) verwendet.

Die Kodierung in UTF-8 hat eine variable Länge von 1 – 4 Byte. Die ersten 128 Zeichen (US-ASCII) werden in einem Byte kodiert. Für Umlaut, Akzent, griechische, arabische und andere Schriftsätze werden zwei Bytes verwendet. Mit drei und vier Bytes können praktisch alle weltweit geläufigen Zeichen dargestellt werden.

1.1.2 Header

Die Vorratsdaten gemäß § 102a Abs. 2 bis 4 TKG 2003 können in fünf Datenarten unterteilt werden:

Nummer	Datenart	gesetzliche Grundlage
1	Internetzugangsdienste	§ 102a Abs. 2 Z 1 - 4 TKG
2	Öffentliche Telefondienste	§ 102a Abs. 3 Z 1 - 6 TKG
3	Erstaktivierung	§ 102a Abs. 3 Z 6c TKG
4	E-mail Verkehrsdaten	§ 102a (4) Z 1 - 4 TKG
5	E-Mail An-/Abmeldung	§ 102a (4) Z 5 TKG

Als erste Zeile jeder Datei wird ein Header eingefügt. Dieser Header enthält die Namen der Datenfelder in dieser Datei. Für jede Datenart gibt es eine spezifische Kopfzeile. In einer Datei dürfen nur Records ein und derselben Datenart enthalten sein. Jeder Datensatz einer Datei hat daher die gleiche Struktur. Die ersten Felder jeder Datei und jedes Records geben Auskunft über Referenz und Abfragekriterium (in dieser Richtlinie als „Indikator“ bezeichnet). Danach kommen die datenartspezifischen Felder. Datenfelder werden im folgenden Text in der Schriftart `Courier New` dargestellt.

1.1.3 Datenfeld „Referenz“

Das erste Datenfeld jeder Datei ist die `Referenz`, die eine eindeutige Referenz zum Auskunftsbegehren („unique ID“ gemäß § 14 DSVO-TKG) und einem bestimmten Betreiber enthält. Diese wird von der Durchlaufstelle vergeben. Die „unique Id“ ist Inhalt des ersten Datenfeldes in jeder Dateiart und jedem Record. Bezieht sich ein Auskunftsbegehren auf mehrere Anbieter, so sind mehrere Bezeichnungen zu vergeben.

Gemäß § 3 DSVO-TKG kann es Fälle geben, bei denen die Übermittlung des Auskunftsbegehrens wegen hoher Dringlichkeit nicht über die DLS (i.a. telefonisch) erfolgt. Eine Nachreichung der Anfrage über die DLS ist in § 3 Abs. 2 DSVO-TKG vorgesehen. Es muss aber sichergestellt werden, dass eine Beantwortung bereits vor der Übermittlung der Anfrage via DLS durchgeführt werden kann. Dazu wird

ein Betreiber-spezifischer Bereich von Referenzen definiert, der vom Betreiber in aufsteigender Reihenfolge vergeben wird.

1.1.4 Datenfeld „IndikatorArt“ und „Indikator“

Nach der Referenz wird bei jeder Dateiart in jedem Record die Art des Indikators und der Indikator selbst angeführt. Damit sind in jeder „csv“-kodierten Datei alle Informationen zur Zuordnung zu einer bestimmten Abfrage enthalten. Der Indikator ist jenes Datum, welches von der abfrageberechtigten Stelle übermittelt wird und zu dem die entsprechenden Daten gesucht werden.

1.1.5 Indikator, Anschlusskennung und Teilnehmerkennung

Indikator, Anschlusskennung und Teilnehmerkennung zeigen auf Identifikationsmerkmale, die anbieter- und anlassspezifisch eingesetzt werden. In der folgenden Tabelle sind die Identifikationsmerkmale und deren Kodierung zusammengefasst. Der Code ist Inhalt der Felder `IndikatorArt`, `AnschlusskennungArt` und `TeilnehmerArt`

Identifikationsmerkmal	Code	Beschreibung
Festnetznummer	NR	E.164 Nummer eines Festnetzbetreibers
MSISDN	MSIS	E.164 Nummer eines Mobilfunkbetreibers
Zielrufnummer	ZIEL	E.164 Rufnummer
IMSI	IMSI	Kennung einer Mobilfunk Subskription nach E.212
IMEI	IMEI	Identifikation eines Mobilfunkendgerätes
Öffentliche IP-Adresse	IP	Identifikation eines Endpunktes in einem Datennetz
Betreiberspezifische Kennung	KENN	Kennung, die nur innerhalb eines Betreibers eindeutig ist. Diese Kennung kann, aber muss nicht, dem Kunden bekannt sein
Cell-Id	CELL	betreiberspezifische Kennung einer Funkzelle
E-Mail Adresse	MAIL	Identifikation eines e-Mail Postfaches

Die folgende Tabelle beschreibt, bei welcher Datenart welche Identifikationsmerkmale als Indikator zur Anwendung kommen können.

Identifikationsmerkmal als Indikator	Datenart				
	1	2	3	4	5
Festnetznummer	X	X			
MSISDN	X	X	X		
Zielrufnummer		X			
IMSI		X			
IMEI		X			
Öffentliche IP-Adresse	X				
Betreiberspezifische Kennung	X				
Cell-Id		X			
E-Mail Adresse				X	X

Bei der Datenart Internetzugangsdienste ist gemäß § 102a. Abs. 2 Z 4 TKG 2003 die eindeutige Kennung des Anschlusses, über den der bestimmte Internetzugang erfolgt ist, aufzuzeichnen. Die Art dieser Anschlusskennung hängt vom Anbieter ab. Im Datensatz werden die Datenfelder `Anschlusskennung` und `AnschlusskennungArt` verwendet. Mögliche Identifikationsmerkmale für die

Anschlusskennung sind Festnetznummer, MSISDN, öffentliche IP-Adresse und betreiberspezifische Kennung.

Bei den Datenarten e-Mail Verkehrsdaten und e-Mail An-/Abmeldung ist gemäß § 102a Abs. 2 Z 1 und Abs. 4 Z 1 die Teilnehmerkennung aufzuzeichnen. Die Art dieser Teilnehmerkennung hängt vom Anbieter ab. Im Datensatz werden die Datenfelder `Teilnehmerkennung` und `TeilnehmerkennungArt` verwendet. Mögliche Identifikationsmerkmale für die Teilnehmerkennung sind Festnetznummer, MSISDN und betreiberspezifische Kennung.

1.1.6 Quelle und Ziel öffentlicher Telefondienste

Im Datensatz für öffentliche Telefondienste werden Quelle und Ziel der Verbindung aufgezeichnet. Bei Abfragen von Mobilfunkanschlüssen werden die jeweils fehlenden Daten IMSI, IMEI oder MSISDN zum Indikator ergänzt. Wird also nach Indikator „`MSISDN`" abgefragt, so werden `IndikatorIMSI` und `IndikatorIMEI` ergänzt.

In den Datensätzen wird jeweils der Partner der Verbindung (der Anrufer bei ankommenden oder das Ziel bei abgehenden Verbindungen) angegeben. Hier werden die Datenfelder `PartnerIMSI`, `PartnerIMEI` und `PartnerMSISDN` verwendet. Die Kodierung von IMSI und IMEI sind den aktuellen ETSI 3GPP Spezifikationen zu entnehmen. Anrufumleitungen können etweder in einem Datensatz oder in zwei Datensätzen dargestellt werden. Wird ein Datensatz verwendet, so enthält das Feld `Anrufumleitung` die Festnetznummer oder die MSISDN des Umleiteziels. Werden zwei Datensätze verwendet, so enthält der zweite Datensatz (Richtung = Aktiv) die Eintragung JA im Datenfeld `Anrufumleitung`.

1.1.7 Ruftyp

Der Ruftyp bei öffentlichen Telefondiensten wird im Datenfeld `Ruftyp` kodiert:

Ruftyp	`Ruftyp`
Telefonie	T
SMS	S
MMS	M

1.1.8 Richtung

Die Richtung des Verbindungsaufbaues wird bei öffentlichen Telefondiensten im Feld `Richtung` angegeben.

Richtung	`Richtung`
Aktiv	A
Passiv	P

1.1.9 Datumsformate

Datum, Uhrzeit und Zeitzone werden in einem Datenfeld dargestellt und nach ISO 8601 kodiert. Folgende Felder sind auf diese Art kodiert: Zeit, Anmeldung und Abmeldung.

Beispiel: Bei Verwendung des Kalendertages und der Uhrzeit mit Winterzeit in Österreich wird der 7. Januar 2010, 9:00 Uhr wie folgt dargestellt: 2010-01-07T09:00:00+01

1.1.10 Rufnummernformate

Rufnummern (nach E.164) werden im Format

„CC NDC Teilnehmernummer"

angegeben. Diese Kodierung wird für die Felder `Festnetznummer, MSISDN, IndikatorMSISDN, Zielrufnummer` und `PartnerMSISDN` verwendet.

CC … Country Code (für Österreich „43")

NDC … National Destination Code („1" für Wien)

1.1.11 Geografische Koordinaten

Die Darstellung geografischer Koordinaten für den Standort des Senders erfolgt nach dem World Geodetic System 1984 (WGS 84). Ob die Darstellung in Graddezimal oder GradMinutenSekunden erfolgt, wird im Einvernehmen mit den Behörden festgelegt.

1.1.12 BetreiberId und CellId

Zur Kennzeichnung von Funkzellen wird das Datenfeld `CellId` verwendet. Die Kodierung dieses Datenfeldes ist netzbetreiberspezifisch. Innerhalb eines Netzbetreibers ist die CellId eindeutig. Die BetreiberId besteht aus Mobile Country Code (MCC) und Mobile Network Code (MNC) gemäß dem Nummerierungsplan nach E.212. Die jeweils aktuelle Liste der vergebenen Betreiber-ID ist bei der RTR-GmbH abrufbar.

1.1.13 E-Mail Adresse

E-Mail Adressen haben die Struktur „local-part@domain“. Die Syntax ist in RFC 5322 und 5321 beschrieben. Das betrifft die Felder `Indikator`, wenn `IndikatorArt` = „MAIL“ ist und die Felder `GesendetAbsender, GesendetEmpfänger, EmpfangAbsender` und `EmpfangZiel`.

1.1.14 IP-Adresse

IPv4-Adressen werden im Format x.x.x.x angegeben, wobei x eine Zahl zwischen 0 und 255 sein kann. IPv6-Adressen hingegen werden im Format x:x:x:x:x:x:x:x angegeben, wobei x eine hexadezimale Zahl zwischen 0 und FFFF sein kann. Die verkürzte Darstellungsvariante bei mehreren aufeinander folgenden 0 mit „::“ gem. IETF RFC 1924 wird nicht verwendet. Die Unterscheidung der Adressformate (IPv4 und IPv6) erfolgt an Hand der unterschiedlichen Darstellungsformen.

Dies betrifft die Datenfelder `Indikator, Anschlusskennung`, falls die `IndikatorArt` bzw. `AnschlusskennungArt` = „IP“ ist. Weiters werden IP-Adressen bei e-Mail Verkehr aufgezeichnet: `GesendetAbsenderIP_Adresse, EmpfangIP_Adresse` und `IP_Adresse`.

1.1.15 Stammdaten

Stammdaten (Vorname, Familienname und Adresse) sind frei beschreibbare Felder. Das betrifft folgende Datenfelder:

- `Vorname, Familienname, Adresse`
- `IndikatorVorname, IndikatorFamilienname, IndikatorAdresse`
- `PartnerVorname, PartnerFamilienname, PartnerAdresse`

1.1.16 Dateiname

Der Dateiname besteht aus dem Datenfeld `Referenz` und ist mit der Dateierweiterung „.csv“ versehen. Werden bei einer Anfrage mehrere Antwort-Files zur gleichen Referenz erstellt, so werden die einzelnen „csv“-Files durchnummeriert (Referenz_1.csv, Referenz_2.csv, etc.).

1.1.17 Nicht ausgefüllte Felder

Je Datenart wird eine Struktur definiert. Allerdings werden in einem Auskunftsbegehren nur bestimmte Datenfelder angefragt. Andererseits müssen bei einem Betreiber nicht alle Datenfelder vorhanden sein. Um diese beiden Fälle im „csv“ File kennzeichnen und unterscheiden zu können, wird festgelegt:

- Datenfelder, die für die Abfrage nicht relevant sind oder nicht nachgefragt wurden, werden mit „#“ (Hexadezimal 23) gefüllt. Dies gilt auch für Daten, die der Betreiber nicht haben kann (z. B. Stammdaten einer Zielrufnummer in einem Fremdnetz).

- Datenfelder, die angefragt wurden, aber beim Betreiber nicht verfügbar sind, werden mit „n.a.“ (für „not available“) gefüllt.

Um Dateninhalte von den Kennzeichen zu unterscheiden, werden diese nicht unter Hochkomma gesetzt. Mit dieser Festlegung wird erreicht, dass der Datenbestand je Datenart einheitlich und daher die Verarbeitung einfacher ist. Datenfelder werden insbesondere dann mit „n.a.“ gefüllt, wenn die betreffenden Daten vom Betreiber nicht erzeugt oder verarbeitet wurden. Im Folgenden werden Beispiele dazu aufgezählt:

-- Die CellId sowie die geografischen Koordinaten werden beim Ruftyp MMS (Multimedia Messaging Service) bei allen Netzbetreibern nicht aufgezeichnet.

-- Falls die Erstaktivierung direkt in der Verkaufsstelle ohne Einbuchen der MSISDN im Netz erfolgt, werden keine geografischen Koordinaten aufgezeichnet.

-- Bei Abfragen nach Kapitel 2.5 e-Mail – An-/Abmeldung wird bei einigen Betreibern das Abmeldedatum nicht aufgezeichnet.

2. Datenarten

Zur Übermittlung der Daten nach § 94 Abs. 4 werden fünf unterschiedliche Datenarten und Datenstrukturen definiert. Damit können alle Auskunftsbegehren beantwortet werden. Diese Datenstrukturen sind die Maximalausprägung der Daten für die jeweiligen Datenarten.

Zu jeder Datenart wird für jedes Abfragekriterium („Indikator“) ein konkreter Anwendungsfall definiert. In Abhängigkeit von diesen Anwendungsfällen werden die möglichen Parameter in den Datenfeldern und die auszufüllenden Felder festgelegt.

2.1 Internetzugangsdienste

Abfragen im Zusammenhang von Internetzugangsdiensten sind vorgesehen um den Zusammenhang zwischen öffentlichen IP-Adressen und Teilnehmern herzustellen. Eine Abfrage nach öffentlichen IP-Adressen liefert jenen Teilnehmer, dem diese IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war. Umgekehrt kann auch abgefragt werden, welche öffentliche IP-Adresse einem bestimmten Teilnehmer zu einem bestimmten Zeitpunkt zugeordnet war.

Grundlage:

§ 92 (3) 3. „Stammdaten“ alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

Name (Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),

akademischer Grad bei natürlichen Personen,

Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen).

§ 92. (3) 6b. „Vorratsdaten“ Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden;

§ 92. (3) 14. „Internet-Zugangsdienst“ einen Kommunikationsdienst im Sinne von § 3 Z 9, der in der Bereitstellung von Einrichtungen oder Diensten zur Erbringung von Zugangsleistungen zum Internet besteht;

§ 92. (3) 16. „Öffentliche IP-Adresse“ eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann. Öffentliche IP-Adressen sind Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a. Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs. 3 Z 3.

§ 102a. (2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:

Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;

Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internetzugangsdienst unter Angabe der zugrundeliegenden Zeitzone;

die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;

die eindeutige Kennung des Anschlusses über den der Internet-Zugang erfolgt ist.

Das Datenformat für die Abfrage von Vorratsdaten zu Internetzugangsdiensten wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
`Referenz`		siehe Kapitel 1.1.3
`IndikatorArt`	NR, MSIS, IP, KENN	siehe Kapitel 1.1.4
`Indikator`	Festnetznummer, MSISDN, IP-Adresse, betreiberspezifische Kennung	
`AnschlusskennungArt`	NR, MSIS, IP, KENN	siehe Kapitel 1.1.5
`Anschlusskennung`	Festnetznummer, MSISDN, IP-Adresse,	

	betreiberspezifische Kennung	
Vorname	optional: akademischer Grad vorangesetzt	siehe Kapitel 1.1.15
Familienname	optional: akademischer Grad vorangesetzt	
Adresse	Präferiert ist die Wohnadresse. Falls diese nicht zur Verfügung steht, wird die Rechnungsadresse eingetragen.	

Falls der Provider aus Mangel an öffentlichen IP-Adressen eine NAT1 anbietet (d.h. zu einer öffentlichen IP-Adresse kann nur eine Menge von möglichen Teilnehmern ermittelt werden), so wird an den Auftraggeber ausschließlich die Information übermittelt, dass eine Einschränkung auf eine bestimmte Person nicht möglich ist.

2.1.1 Indikator IP-Adresse

Bei Abfrage nach IP-Adresse wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 1.1.3
IndikatorArt	IP	siehe Kapitel 1.1.4
Indikator	IP Adresse	
AnschlusskennungArt	KENN, NR, MSIS	siehe Kapitel 1.1.5
Anschlusskennung	betreiberspezifische Kennung, Festnetznummer, MSISDN	
Vorname	optional: akademischer Grad vorangesetzt	siehe Kapitel 1.1.15
Familienname	optional: akademischer Grad vorangesetzt	
Adresse	Präferiert ist die Anschlussadresse. Falls diese nicht zur Verfügung steht, wird die Rechnungsadresse eingetragen.	

Die Abfrage gibt Auskunft darüber, wem eine bestimmte öffentliche IP-Adresse zu einem bestimmten Zeitpunkt zugeteilt war. Die Art der Anschlusskennung hängt vom Betreiber ab (Mobilfunk – MSISDN, Festnetzbetreiber/Kabelnetzbetreiber/ISP – betreiberspezifische Kennung oder Telefonnummer bzw. Dial-up Nummer). Jeder Anschlusskennung werden – falls möglich – die betreffenden Stammdaten zugeordnet.

2.1.2 Indikator Teilnehmerkennung

Bei Abfrage nach Teilnehmerkennung wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 1.1.3
IndikatorArt	KENN, NR, MSIS	siehe Kapitel 1.1.4
Indikator	betreiberspezifische Kennung, Festnetznummer, MSISDN	
AnschlusskennungArt	IP	siehe Kapitel 1.1.5
Anschlusskennung	IP-Adresse	
Vorname	#	
Familienname	#	

1 Mit einer NAT (Network Address Translation) wird die öffentliche IP-Adresse dynamisch Adressen eines privaten Adressraumes zugeordnet.

Adresse	#	

Die Abfrage gibt Auskunft darüber, welche IP-Adresse einem bestimmten Teilnehmer zu einem bestimmten Zeitpunkt zugeordnet war. Die Art des Indikators hängt vom Betreiber ab und wird in den meisten Fällen eine Telefonnummer (Festnetznummer oder MSISDN) sein. In diesem Fall werden Stammdaten nicht ausgefüllt.

2.2 Öffentliche Telefondienste

Die Vorratsdatenspeicherung für öffentliche Telefondienste umfasst aktive und passive Gespräche sowie Informationen über Gesprächspartner. Besondere Abfragen können nach Cell-Id und Zielrufnummer gestellt werden.

Grundlage:

§ 92. (3) 6a. „Standortkennung“ die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-Id);

§ 92. (3) 8. „Anruf“ eine über einen öffentlichen Telefondienst aufgebaute Verbindung, die eine zwei- oder mehrseitige Echtzeit-Kommunikation ermöglicht;

§ 92. (3) 8a. „erfolgloser Anrufversuch“ einen Telefonanruf, bei dem die Verbindung erfolgreich aufgebaut wurde, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat;

§ 92. (3) 10. „elektronische Post“ jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

§ 92. (3) 13. „Internet-Telefondienst“ einen öffentlichen Telefondienst im Sinne des § 3 Z 16, der auf paketvermittelter Nachrichtenübertragung über das Internet-Protokoll basiert;

§ 102a. (3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:

Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;

bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;

Name und Anschrift des anrufenden und des angerufenen Teilnehmers;

Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;

die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste);

Betreibern von Mobilfunknetzen obliegt zudem die Speicherung

der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;

der internationalen Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses;

Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;

der Standortkennung (Cell-ID) bei Beginn einer Verbindung;

Das Datenformat für die Abfrage von Vorratsdaten zu öffentlichen Telefondiensten wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 1.1.3
IndikatorArt	NR, MSIS, ZIEL, IMSI, IMEI, CELL	siehe Kapitel 1.1.4
Indikator	Festnetznummer, MSISDN, Zielrufnummer, IMSI, IMEI, Cell-Id	
IndikatorMSISDN		siehe Kapitel 1.1.6
IndikatorIMSI		
IndikatorIMEI		

IndikatorVorname		siehe Kapitel 1.1.15
IndikatorFamilienname		
IndikatorAdresse		
BetreiberId	diese Information bezieht sich auf den Indikator und ist nur für Mobilfunkbetreiber relevant	siehe Kapitel 1.1.12
CellId	die CellId ist Netzbetreiber-spezifisch	
GeoKoordinaten	das sind die geografischen Koordinaten des Senderstandortes	siehe Kapitel 1.1.11
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 1.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 1.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 1.1.8
PartnerMSISDN		siehe Kapitel 1.1.6
PartnerIMSI	IMSI und IMEI werden nur angegeben, wenn sich der Partner im eigenen (Mobilfunk-) Netz befindet.	
PartnerIMEI		
PartnerVorname	Die Stammdaten können nur ermittelt werden, wenn sich der Partner im eigenen Netz befindet.	siehe Kapitel 1.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt (JA) oder enthält die Zielrufnummer der Anrufumleitung	siehe Kapitel 1.1.6

Wird das Auskunftsbegehren für einen Namen oder eine Adresse gestellt, so erhebt der Betreiber die in Frage kommenden Indikatoren und führt die Abfrage nach diesen Indikatoren durch. Nicht erfolgreiche Verbindungen werden nur in dem Ausmaß erfasst, als der Betreiber dies auch bisher durchgeführt hat (§ 102a Abs. 5 TKG 2003). Eine separate Kennzeichnung zur Unterscheidung von erfolgreichen und nicht erfolgreichen Verbindungen gibt es nicht.
Anrufumleitung bezieht sich auf eine aktivierte Anrufumleitung durch den Indikator. Für Anrufumleitung können zwei Gesprächsdatensätze im „csv“ File enthalten sein. Die erste Verbindung geht vom Partner zum Indikator und die zweite vom Indikator zum Umleiteziel. Der zweite Datensatz ist als umgeleitete Verbindung gekennzeichnet (Anrufumleitung = ja). Optional besteht auch die Möglichkeit, nur einen Datensatz aufzuzeichnen und das Umleiteziel im Feld Anrufumleitung einzutragen. Die Information, ob es sich um ein Fax oder Datentransfer via Modem handelt, kann aus technischen Gründen nicht inkludiert werden.
Ein Internet-Telefondienst ist gemäß § 92 (3) Z 13 ein „öffentlicher Telefondienste“ iSd § 3 Z 16 TKG. Im Sinne dieser Bestimmung ist VoIP Klasse A iSd Richtlinien für Anbieter von VoIP Diensten der RTR zu verstehen. Diese Internet-Telefondienste werden in der gleichen Form beauskunftet wie andere öffentliche Telefondienste.

2.2.1 Indikator Festnetznummer
Bei Abfrage nach Festnetznummer wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 1.1.3
IndikatorArt	NR	siehe Kapitel 1.1.4
Indikator	Festnetznummer	
IndikatorMSISDN	#	

IndikatorIMSI	#	
IndikatorIMEI	#	
IndikatorVorname	#	
IndikatorFamilienname	#	
IndikatorAdresse	#	
BetreiberId	#	
CellId	#	
GeoKoordinaten	#	
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 1.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 1.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 1.1.8
PartnerMSISDN	die Rufnummer des Partners	siehe Kapitel 1.1.6
PartnerIMSI	#	
PartnerIMEI	#	
PartnerVorname	Die Stammdaten können nur ermittelt werden, wenn sich der Partner im eigenen Netz befindet.	siehe Kapitel 1.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt oder enthält optional die Zielrufnummer der Anrufumleitung	siehe Kapitel 1.1.6

2.2.2 Indikator MSISDN, IMEI oder IMSI

Bei Abfrage nach MSISDN, IMSI oder IMEI wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 1.1.3
IndikatorArt	MSIS, IMSI, IMEI	siehe Kapitel 1.1.4
Indikator	MSISDN, IMSI oder IMEI	
IndikatorMSISDN	Die jeweils fehlenden Daten zum Indikator werden eingetragen.	siehe Kapitel 1.1.6
IndikatorIMSI		
IndikatorIMEI		
IndikatorVorname	#	
IndikatorFamilienname	#	
IndikatorAdresse	#	
BetreiberId	Id des Netzbetreibers, in dem sich der Indikator befindet	siehe Kapitel 1.1.12
CellId	CellId, in dem sich der Indikator bei Beginn der Verbindung befindet	
GeoKoordinaten	geografische Koordinaten des Senderstandortes, in dem sich der Indikator zu Beginn der Verbindung befindet	siehe Kapitel 1.1.11
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 1.1.9
Dauer	in Sekunden	Zahl

Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 1.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 1.1.8
PartnerMSISDN	die Rufnummer des Partners	siehe Kapitel 1.1.6
PartnerIMSI	Diese Daten werden nur eingetragen, wenn sich der Partner im eigenen Netz befindet.	
PartnerIMEI		
PartnerVorname	Die Stammdaten können nur ermittelt werden, wenn sich der Partner im eigenen Netz befindet.	siehe 1.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt oder enthält optional die Zielrufnummer der Anrufumleitung	siehe 1.1.6

Bei Roaming in anderen Netzen wird die jeweilige BetreiberId angegeben. In diesen Fällen sind die Felder CellId und GeoKoordinaten nicht ausgefüllt (#). Bei Roaming werden die Gesprächsdaten von jenem Betreiber aufgezeichnet, in dessen Netz sich der Teilnehmer aufhält. Die Übermittlung dieser Gesprächdaten zum Heimatnetzbetreiber kann einige Zeit in Anspruch nehmen. Bei der Abfrage werden daher nur jene Daten erfasst, die zum Zeitpunkt der Abfrage vorliegen. Es ist nicht sichergestellt, dass alle Roamingdaten enthalten sind.
Bei Network Sharing, MVNO und nationalem Roaming schickt die Behörde das Auskunftsbegehren an alle involvierten Netzbetreiber, um eine vollständige Datenerfassung sicherzustellen.

2.2.3 Indikator CellId
Bei Abfrage nach CellId wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 1.1.3
IndikatorArt	CELL	siehe Kapitel 1.1.4
Indikator	Cell-Id	
IndikatorMSISDN	Hier werden Informationen über die Teilnehmer eingetragen, die sich in der abgefragten Zelle in dem abgefragten Zeitraum aufgehalten haben und/oder Verbindungen aufgebaut haben.	siehe Kapitel 1.1.6
IndikatorIMSI		
IndikatorIMEI		
IndikatorVorname		siehe Kapitel 1.1.15
IndikatorFamilienname		
IndikatorAdresse		
BetreiberId	Id des Netzbetreibers, in dem sich der Indikator befindet	siehe Kapitel 1.1.12
CellId	CellId, in dem sich der Teilnehmer bei Beginn der Verbindung befindet	
GeoKoordinaten	geografische Koordinaten des Senderstandortes, in dem sich der Teilnehmer zu Beginn der Verbindung befindet	siehe Kapitel 1.1.11
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 1.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 1.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 1.1.8
PartnerMSISDN	die Rufnummer des Partners	siehe Kapitel

PartnerIMSI	Diese Daten werden nur eingetragen, wenn sich der Partner im eigenen Netz befindet.	1.1.6
PartnerIMEI		
PartnerVorname	Die Stammdaten können nur ermittelt werden, wenn sich der Partner im eigenen Netz befindet.	siehe Kapitel 1.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt oder enthält optional die Zielrufnummer der Anrufumleitung	siehe Kapitel 1.1.6

Mit dieser Abfrage soll festgestellt werden, welche Mobilfunkteilnehmer/-geräte zu einer bestimmten Zeit in einem bestimmten geografischen Bereich Verbindungen aufgebaut haben.
Falls verfügbar, werden die Stammdaten sowohl des Teilnehmers in dieser Zelle als auch des Partners angegeben. Für Teilnehmer aus fremden Netzen (Visitor Roaming) können Stammdaten nicht inkludiert werden. Falls sich das Auskunftsbegehren an einen bestimmten geografischen Bereich richtet, erhebt der Netzbetreiber, welche Zellen dafür in Frage kommen und führt die Abfrage je CellId durch.

2.2.4 Indikator Zielrufnummer
Bei Abfrage nach Zielrufnummer wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 1.1.3
IndikatorArt	ZIEL	siehe Kapitel 1.1.4
Indikator	Zielrufnummer	
IndikatorMSISDN	#	siehe Kapitel 1.1.6
IndikatorIMSI	#	
IndikatorIMEI	#	
IndikatorVorname	#	siehe Kapitel 1.1.15
IndikatorFamilienname	#	
IndikatorAdresse	#	
BetreiberId	#	
CellId	#	
GeoKoordinaten	#	
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 1.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 1.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 1.1.8
PartnerMSISDN	Hier werden Informationen über die Teilnehmer eingetragen, die Verbindungen zu dieser Zielrufnummer aufgebaut haben.	
PartnerIMSI		
PartnerIMEI		
PartnerVorname		
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	#	

Zweck dieser Abfrage ist es, festzustellen, welche Teilnehmer diese Zielrufnummer gerufen haben. Es handelt sich dabei immer um eine Zielrufnummer in einem Fremdnetz (sonst würde eine Abfrage nach Kapitel 0 oder 0 gestellt werden). Die Abfrage kann an Festnetz- oder an Mobilfunkbetreiber gestellt werden. Es sind die jeweils relevanten Daten auszufüllen. Die jeweilige Rufnummer ist im Feld PartnerMSISDN einzutragen. Standortdaten werden bei dieser Abfrage nicht inkludiert. Diese müssten in einem zweiten Schritt nach Kapitel 0 abgefragt werden.

2.3 Erstaktivierung

Diese Datenstruktur erlaubt die Übermittlung von Datum und Uhrzeit der Erstaktivierung bei vorbezahlten anonymen Diensten.

Grundlage:

§ 102a. (3) Anbietern öffentlicher Telefondienste obliegt die Speicherung folgender Daten:

Betreibern von Mobilfunknetzen obliegt zudem die Speicherung

Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anoynme Dienste handelt;

Das Datenformat für die Abfrage von Vorratsdaten zur Erstaktivierung wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
`Referenz`		siehe Kapitel 1.1.3
`IndikatorArt`	MSIS	siehe Kapitel 1.1.4
`Indikator`	MSISDN	
`BetreiberId`	Id des Netzbetreibers	siehe Kapitel 1.1.12
`CellId`	CellId, in dem der Teilnehmer die Erstaktivierung durchgeführt hat	
`GeoKoordinaten`	geografische Koordinaten des Senderstandortes, in dem der Teilnehmer die Erstaktivierung durchgeführt hat	siehe Kapitel 1.1.11
`Zeit`	Datum und Uhrzeit der Erstaktivierung	siehe Kapitel 1.1.9

Die Beauskunftung darf nur erfolgen, wenn die Erstaktivierung nicht länger als 6 Monate zurückliegt.

2.4 E-Mail – Verkehrsdaten

Zweck dieses Datenformates ist Auskunft über E-Mail Verkehr. Dabei werden zu einer bestimmten E-Mail Adresse die Absender ankommender E-Mails und die Zieladressen gesendeter E-Mails angegeben.

Grundlage:

§ 92. (3) 2b „E-Mail Adresse“ die eindeutige Kennung, die einem elektronischen Postfach von einem Internet E-Mail Anbieter zugewiesen wird;

§ 92. (3) 10. „elektronische Post“ jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

§ 92. (3) 11. „elektronisches Postfach“ ein elektronisches Ablagesystem, das einem Teilnehmer eines E-Mail Dienstes zugeordnet ist;

§ 92. (3) 12. „E-Mail“ elektronische Post, die über das Internet auf Basis des „Simple Mail Transfer Protokoll“ (SMTP) versendet wird;

§ 92. (3) 15. „E-Mail Dienst“ einen Kommunikationsdienst im Sinne von § 3 Z 9, welcher den Versand und die Zustellung von E-Mails auf Basis des „Simple Mail Transfer Protokoll“ (SMTP) umfasst;

§ 102a. (4) Anbietern von E-Mail Diensten obliegt die Speicherung folgender Daten:

die einem Teilnehmer zugewiesene Teilnehmerkennung;

Name und Anschrift des Teilnehmers, dem eine E-Mail Adresse zu einem bestimmten Zeitpunkt zugewiesen war;

bei Versenden einer E-Mail die E-Mail Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail Adresse jedes Empfängers der E-Mail;

beim Empfang einer E-Mail und deren Zustellung in ein elektronisches Postfach die E-Mail Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung;
Das Datenformat für die Abfrage von Vorratsdaten bezüglich E-Mail Verkehr wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
`Referenz`		siehe Kapitel 1.1.3
`IndikatorArt`	MAIL	siehe Kapitel 1.1.4
`Indikator`	E-Mail Adresse	
`TeilnehmerkennungArt`	NR, MSIS, KENN	siehe Kapitel 1.1.5
`Teilnehmerkennung`	Festnetznummer, MSISDN, betreiberspezifische Kennung	
`Zeit`	Datum, Uhrzeit und Zeitzone nach ISO 8601	siehe Kapitel 1.1.9
`GesendetAbsender`	Bei gesendeten E-Mails wird je Adressat ein Datensatz aufgenommen.	siehe Kapitel 1.1.13
`GesendetAbsenderIP Adresse`		siehe Kapitel 1.1.14
`GesendetEmpfänger`		siehe Kapitel 1.1.13
`EmpfangAbsender`	Bei empfangenen E-Mails wird die E-Mail Adresse des Absenders und jene des Empfängers angegeben.	siehe Kapitel 1.1.13
`EmpfangZiel`		siehe Kapitel 1.1.13
`EmpfangIP_Adresse`	öffentliche IP-Adresse der letztübermittelnden Kommunikationseinrichtung	siehe Kapitel 1.1.14

Es wird nur die jeweils im Auskunftsbegehren angegebene E-Mail Adresse abgefragt. Für Aliases müssen eigene Auskunftsbegehren gestellt werden. Falls ein Betreiber nur einen Server für abgehende E-Mails anbietet, sind nur Informationen über diese E-Mails in die Abfrage aufzunehmen. Der vollständige E-Mail Verkehr kann in diesem Fall nur durch Abfrage bei beiden Betreibern (dem, in dessen Zuständigkeitsbereich der Server für abgehende E-Mails steht und jener, in dessen Zuständigkeitsbereich der Server für ankommend E-Mails steht) ermittelt werden.

Datum/Uhrzeit wird aus den Log-Einträgen des Mail-Servers entnommen. Bei gesendeten E-Mails gibt dieser Zeitstempel an, wann die E-Mail vom Client im E-Mail Server erhalten wurde. Bei empfangenen E-Mails gibt der Zeitstempel den Zeitpunkt des Einlangens beim E-Mail-Server an („received“). Die E-Mail Adressdaten des Absenders und der Empfänger stammen vom „MAIL“ und „RCPT“ command der E-Mail iSd RFC 5321. Spam E-Mails, die bereits vor Zustellung in das Postfach vom Betreiber ausgefiltert wurden, werden nicht aufgezeichnet.[2]

E-Mail Alias Adressen, die zum Zeitpunkt der Abfrage nicht mehr aktiv sind, können nicht rückwirkend einem bestimmten Teilnehmer zugeordnet werden. Diese Historisierung wird von den österreichischen Anbietern nicht durchgeführt.[3]

Stammdaten zum E-Mail Verkehr sind in der „csv“-Datei nicht enthalten. Zur Abfrage dieser Daten müsste eine gesonderte Stammdatenabfrage erfolgen. Es wird darauf hingewiesen, dass Absenderinformation (wie bei einem Brief) kein gesichertes Datum darstellt. Eine Manipulation bzw. Verfälschung durch den Teilnehmer ist in einfacher Weise möglich.
Die öffentliche IP-Adresse des Absenders einer E-Mail kann eine NAT bezeichnen und damit keinen eindeutigen Rückschluss auf den Teilnehmer zulassen.

2.5 E-Mail – An-/Abmeldung
Zweck dieses Datenformates ist Auskunft über An- und Abmeldung des Teilnehmers beim E-Mail Server.

Grundlage:

§ 102a. (4) Anbietern von E-Mail Diensten obliegt die Speicherung folgender Daten:

2 siehe auch Erläuterungen zu § 102a Abs. 5
3 siehe auch Erläuterungen zu § 102a Abs. 4 Z 1 und 2

bei An- und Abmeldung beim E-Mail Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrundeliegenden Zeitzone.
Das Datenformat für die Abfrage von An-/Abmeldedaten beim E-Mail Server wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
`Referenz`		siehe Kapitel 1.1.3
`IndikatorArt`	MAIL	siehe Kapitel 1.1.4
`Indikator`	E-Mail Adresse	
`TeilnehmerkennungArt`	NR, MSIS, KENN	siehe Kapitel 1.1.5
`Teilnehmerkennung`	Festnetznummer, MSISDN, betreiberspezifische Kennung	
`Anmeldung`	Datum, Uhrzeit und Zeitzone der Anmeldung	siehe Kapitel 1.1.9
`Abmeldung`	Datum, Uhrzeit und Zeitzone der Abmeldung	siehe Kapitel 1.1.9
`IP Adresse`		siehe Kapitel 1.1.14

Es gibt für die Kunden eines E-Mail Dienstanbieters mehrere Methoden, E-Mails abzurufen. Bei Webmail-Zugang melden sich Kunden üblicherweise nicht explizit ab. Daher ist der Zeitpunkt der Abmeldung in den meisten Fällen das Time-out des E-Mail Servers, nicht aber das Schließen des Browser-Fensters.4 Bei E-Mail Push Services (z. B. Blackberry) muss der Blackberry Server nicht im Einflussbereich des E-Mail Anbieters stehen. Es ist davon auszugehen, dass der Blackberry Server permanent beim E-Mail Server eingeloggt ist.
Die öffentliche IP-Adresse des Absenders einer E-Mail kann eine NAT bezeichnen und damit keinen eindeutigen Rückschluss auf den Teilnehmer zulassen.

4 siehe auch Erläuterungen zu § 102a Abs. 4 Z 5

Beilage

Beispiele zur Definition der Datenfelder

1 Annex Beispiele (informativ und exemplarisch)

Dieser Annex enthält Beispiele für Anwendungsfälle je Datenart und Indikator. Dazu werden jeweils der Header und ein Beispiel für einen Datensatz angegeben. Alle Beispieldaten sind fiktiv (der Wiener Rufnummernbereich 991 sowie die Mobilfunkkennzahlen 663 und 665 sind dzt. nicht zugeteilt, als Domain Namen wurde lt. RFC 2606 example.com verwendet, IP-Adressen wurden aus dem reservierten Bereich 192.0.2.00/24 gemäß RFC 3330 entnommen, Namen und Adressen sind fiktiv).
In Kapitel 5.1 werden die rechtlichen Grundlagen für Anfragen nach TKG, StPO und SPG zusammengefasst. Kapitel 5.2 beschreibt die Auskünfte über Vorratsdaten. Auskünfte über Daten einer Nachrichtenübermittlung haben dieselbe Struktur wie Vorratsdaten (Kapitel 5.3.). In Kapitel 5.4 ff werden diese Anfragen für die Anwendung gemäß § 76a (2) StPO und § 53 (3a) und (3b) SPG spezifiziert.
Generell stellen die Use Cases den Maximalumfang der übermittelten Daten dar. Wenn in der Anfrage eine weitere Einschränkung erfolgt, kann auch die Antwort auf die angefragten Felder eingeschränkt werden.

Rechtliche Grundlagen für Beauskunftung

Die Schnittstelle nach § 94 (4) TKG dient zur Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG. Daher werden zunächst die rechtlichen Grundlagen für die Beauskunftung dieser Daten zusammengefasst.

1.1.1 TKG 2003

Nach § 90 (6) sind Anbieter von Kommunikationsdiensten verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten im Sinne von § 92 Abs. 3 Z 3 lit. a bis e von Teilnehmern zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben, soweit dies ohne Verarbeitung von Verkehrsdaten möglich ist.
Nach § 90 (7) sind Anbieter von Kommunikationsdiensten auf schriftliches Verlangen der zuständigen Gerichte, Staatsanwaltschaften oder der Kriminalpolizei (§ 76a Abs. 1 StPO) verpflichtet, diesen zur Aufklärung und Verfolgung des konkreten Verdachts einer Straftat Auskunft über Stammdaten (§ 92 Abs. 3 Z 3) von Teilnehmern zu geben. Dies gilt sinngemäß für Verlangen der Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 1 SPG. In dringenden Fällen können aber solche Ersuchen vorläufig mündlich übermittelt werden.

1.1.2 StPO – Auskunft über Daten einer Nachrichtenübermittlung und Auskunft über Vorratsdaten auf Grund einer richterlichen Bewilligung

Nach § 134 StPO ist die "Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG) und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes).
"Auskunft über Vorratsdaten" ist die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs. 2 bis 4 TKG zu

speichern haben und die nicht nach § 99 Abs. 2 TKG einer Auskunft nach Z 2 (Auskunft über Daten einer Nachrichtenübermittlung) unterliegen.
In § 135 (2) und (2a) StPO ist die Zulässigkeit der Auskunft über Daten einer Nachrichten–übermittlung und Vorratsdaten normiert.

1.1.3 StPO – Auskunft über Stamm- und Zugangsdaten auf Anordnung der Staatsanwaltschaft

Nach § 76a (2) StPO sind Anbieter von Telekommunikationsdiensten auf Anordnung der Staatsanwaltschaft zur Auskunft über folgende Daten nach § 99 Abs. 5 Z 2 TKG verpflichtet:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war, es sei denn, dass diese Zuordnung eine größere Anzahl von Teilnehmern erfassen würde;

2. die bei Verwendung von E-Mail Diensten dem Teilnehmer zugewiesene Teilnehmer-kennung;

3. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, und

4. die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders einer E-Mail.

1.1.4 SPG - Stammdatenabfrage (Telefonie, IP-Adressen)

Nach § 53 (3a) SPG sind die Sicherheitsbehörden berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskunft zu verlangen:

1. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses, wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist,
2. über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr
   a. einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),
   b. eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder
   c. einer kriminellen Verbindung (§ 16 Abs.1 Z 2) benötigen,
3. über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr,
   a. einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),
   b. eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder
   c. einer kriminellen Verbindung (§ 16 Abs.1 Z 2) benötigen,

auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist,

4. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer, wenn dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe erforderlich ist.

1.1.5 SPG – Standortdaten, Vorratsdaten

Nach § 53 (3b) SPG gilt: "Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen, auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist, sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen."

Use Cases für Auskunft über Vorratsdaten nach § 135 StPO

„Auskunft über Vorratsdaten“ ist die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs. 2 bis 4 TKG zu speichern haben und die nicht nach § 99 Abs. 2 TKG einer Auskunft nach Z 2 (Auskunft über Daten einer Nachrichtenübermittlung) unterliegen“.
Die Daten nach Maßgabe des § 102a wurden in folgende fünf Datenarten unterteilt:

Nummer	Datenart	gesetzliche Grundlage
1	Internetzugangsdienste	§ 102a (2) Z 1 - 4 TKG
2	öffentliche Telefondienste	§ 102a (3) Z 1 - 6
3	Erstaktivierung	§ 102a (3) Z 6 c
4	E-Mail Verkehrsdaten	§ 102a (4) Z 1 - 4
5	E-Mail An-/Abmeldung	§ 102a (4) Z 5

Zur Auskunft über diese Daten sind folgende Use Cases vorgesehen:

1.1.6 Datenart Internetzugangsdienste

1.1.6.1 Indikator IP-Adresse

Anforderung: Auskunft über Vorratsdaten / Internetzugangsdienste zur IP Adresse 192.0.2.0 zu einem bestimmten Zeitpunkt
Dateiname: 100001.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF
"100001","IP","192.0.2.0","KENN","45672000","Max","Mustermann"
,
"1030 Wien, Landstrasse 27" CRLF
```

1.1.6.2 Indikator betreiberspezifische Kennung

Anforderung: Auskunft über Vorratsdaten / Internetzugangsdienste zur Anschlusskennung 45672000 und zu einem bestimmten Zeitpunkt

Dateiname: 100002.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF
"100002","KENN","45672000","IP","192.0.2.0","Max","Mustermann"
,
"1030 Wien, Landstrasse 27" CRLF
```

1.1.6.3 Indikator Festnetznummer

Anforderung: Auskunft über Vorratsdaten / Internetzugangsdienste zur Festnetznummer Wien 991 65 98 und zu einem bestimmten Zeitpunkt

Dateiname: 100003.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF
"100003","NR","4319916598","IP","192.0.2.0","Max","Mustermann"
,
"1020 Wien, Landstrasse 27" CRLF
```

1.1.6.4 Indikator MSISDN

Anforderung: Auskunft über Vorratsdaten / Internetzugangsdienste zur Mobilnummer 0665 312 65 65 und zu einem bestimmten Zeitpunkt

Dateiname: 100004.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF
"100004","MSIS","436653126565","IP","192.0.2.10","Max","Muster
mann",
"1010 Wien, Landstrasse 27" CRLF
```

1.1.7 Datenart öffentliche Telefondienste

1.1.7.1 Indikator Festnetznummer

Anforderung: Auskunft über Vorratsdaten / öffentliche Telefondienste zur Festnetznummer Wien 991 8002 während eines bestimmten Zeitraums

Dateiname: 100005.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","Indik
atorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Ze
it","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI
",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anruf
umleitung" CRLF
"100005","NR","4319918002",#,#,#,#,#,#,#,#,#,
"2010-01-
12T21:23:00+01","412","T","A","436655126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine aktive Telefonverbindung zu einer Mobilfunknummer aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Festnetzbetreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

1.1.7.2 Indikator MSISDN1

Anforderung: Auskunft über Vorratsdaten / öffentliche Telefondienste zur Mobilrufnummer 0665 98 75634 während eines bestimmten Zeitraums
Dateiname: 100006.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","Indik
atorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Ze
it","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI
",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anruf
umleitung" CRLF
"100006","MSIS","436659875634",#,"232031234567890",
"35-209900-176148-1",#,#,#,"T-
Mobile","87543","16.151715/45.758972",
"2010-01-
12T21:23:00+01","42","T","P","436655126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine passive Telefonverbindung zu einer anderen Mobilfunknummer inkl. IMSI, IMEI, Cell-Id und geografische Koordinaten aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Mobilfunknetzbetreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

1.1.7.3 Indikator IMEI

Anforderung: Auskunft über Vorratsdaten / öffentliche Telefondienste zur IMEI 35-209900-176148-1 während eines bestimmten Zeitraums
Dateiname: 100007.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","Indik
atorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Ze
it","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI
",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anruf
umleitung" CRLF
"100007","IMEI","35-209900-176148-1",
"436769875634","232031234567890",#,#,#,#,"T-Mobile","87543",
"16.151715/45.758972","2010-01-12T21:23:00+01","42","T","P",
"436655126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine passive Telefonverbindung zu einer anderen Mobilfunknummer inkl. MSISDN, IMSI, Cell-Id und Geo Koordinaten aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Mobilfunknetzbetreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

---

1 GeoKoordinaten werden in den Beispielen in Graddezimal kodiert.

1.1.7.4 Indikator IMSI

Anforderung: Auskunft über Vorratsdaten / öffentliche Telefondienste zur IMSI 232031234567890 während eines bestimmten Zeitraums
Dateiname: 100008.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","Indik
atorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Ze
it","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI
",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anruf
umleitung" CRLF
"100008","IMSI","232031234567890","436659875634",#,
"35-209900-176148-1",#,#,#,"T-
Mobile","87543","16.151715/45.758972",
"2010-01-
12T21:23:00+01","42","T","P","436635126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine passive Telefonverbindung zu einer anderen Mobilfunknummer inkl. MSISDN, IMEI, Netzbetreiber, Cell-Id und Geo Koordinaten aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Mobilfunknetz-betreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

1.1.7.5 Indikator Cell-Id

Anforderung: Auskunft über Vorratsdaten / öffentliche Telefondienste zur Cell-Id 76465 während eines bestimmten Zeitraums
Dateiname: 100009.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","Indik
atorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Ze
it","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI
",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anruf
umleitung" CRLF
"100009","CELL","76465","436654527634",
"232031234567890","35-209900-176148-1","Max","Mustermann",
"2020 Graz, Wohnstrasse 45","T-
Mobile","76465","16.151715/45.758972",
"2010-01-
12T21:23:00+01","42","T","P","436635126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine Telefonverbindung zwischen zwei Mobilfunk-teilnehmern aufgezeichnet. Zu aktiven Teilnehmer werden MSISDN, IMSI, IMEI, Stammdaten und Geo Koordinaten aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Mobilfunknetzbetreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

1.1.7.6 Indikator Zielrufnummer

Anforderung: Auskunft über Vorratsdaten / öffentliche Telefondienste zur Zielrufnummer Wien 991 5432 während eines bestimmten Zeitraums
Dateiname: 100010.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","Indik
atorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Ze
it","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI
",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anruf
umleitung" CRLF
"100010","ZIEL","4319915432",#,#,#,#,#,#,#,#,#,#,
"2010-01-
12T21:23:00+01","22","T","A","4319914534",#,#,"Max","Musterman
n",
"2322 Baden, Wohnstrasse 45",# CRLF
```

Bemerkung: In diesem Beispiel wird eine Telefonverbindung zu dieser Zielrufnummer von der Wiener Rufnummer 991 4534 aufgezeichnet. Zu dieser Rufnummer sind auch die Stammdaten enthalten. Es handelt sich um ein Aktivgespräch aus Sicht der Rufnummer 991 4534. Die Zielrufnummer befindet sich in einem Fremdnetz.

1.1.8 Datenart Erstaktivierung

Anforderung: Auskunft über Vorratsdaten / Erstaktivierung zur MSISDN 06637543234
Dateiname: 100011.csv

```
"Referenz","IndikatorArt","Indikator","BetreiberId","CellId",
"GeoKoordinaten","Zeit" CRLF
"100011","MSIS","436637543234","Orange","76543",
"16.151715/45.758972","2010-01-12T21:23:00+01" CRLF
```

1.1.9 Datenart E-Mail Verkehrsdaten

Anforderung: Auskunft über Vorratsdaten / E-Mail Verkehrsdaten zur E-Mail Adresse max@example.com während eines bestimmten Zeitraums
Dateiname: 100012.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Zeit","GesendetAbsender","GesendetAbsende
rIP_Adresse",
"GesendetEmpfaenger","EmpfangAbsender","EmpfangZiel","EmpfangI
P_Adresse" CRLF
```

Gesendete E-Mail:

```
"100012","MAIL","max@example.com","NR","4319918767",
"2010-01-12T21:23:00+01","max@example.com","192.0.2.20",
"mona@example.com",#,#,# CRLF
```

Empfangene E-Mail:

```
"100012","MAIL","max@example.com","NR","4319918767",
"2010-01-
12T21:23:12+01",#,#,#,"mona@example.com","max@example.com",
"192.0.2.10" CRLF
```

1.1.10 Datenart E-Mail An-/Abmeldung

Anforderung: Auskunft über Vorratsdaten / E-Mail An-/Abmeldung zur E-Mail Adresse max@example.com während eines bestimmten Zeitraums
Dateiname: 100013.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Anmeldung","Abmeldung",IP_Adresse" CRLF
"100013","MAIL","max@example.com","NR","4319918767",
"2010-01-12T21:23:00+01",#,"192.0.2.5" CRLF
```

1.1.11 Beispiel für Auskunft über mehrerer Daten

Am 2. Februar 2010 wird unter der Referenz 100014 eine Anfrage nach den Indikatoren MSISDN 0663 8752368 sowie 0665 7646893 und der Datenart Internetzugangsdienste gestellt.
Als Ergebnis werden zwei "csv"-Files mit folgenden Dateinamen erzeugt:
Dateiname 1: 100014_1.csv
Dateiname 2: 100014_2.csv

Auskunft über Daten einer Nachrichtenübermittlung

Nach § 134 StPO gehören dazu Verkehrsdaten, Zugangsdaten und Standortdaten:
§ 92 (3) Z 4 TKG: “Verkehrsdaten” Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;
§ 92 (3) Z 4a TKG: “Zugangsdaten” jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind;
§ 92 (3) Z 6 TKG: “Standortdaten” Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben;
Die Auskunft über Daten einer Nachrichtenübermittlung betrifft eine Untermenge der Daten, die als Vorratsdaten erfasst werden Daher kommen für die Beauskunftung die gleichen Use Cases zur Anwendung wie auch für Vorratsdaten. Dabei sind allerdings die Bestimmungen über die Zulässigkeit der Datenspeicherung zu beachten.
Nach § 99 (1) TKG dürfen Verkehrsdaten außer in den gesetzlich geregelten Fällen nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Nach § 99 (2) TKG gilt: *"Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken."*
Die konkrete Speicherdauer hängt vom Geschäftsmodell und den betrieblichen Notwendigkeiten des jeweiligen Netzbetreibes ab.

Auskunft nach § 76a (2) Z 1 StPO

Es sind nach § 76a (2) Z 1 StPO zu beauskunften: Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war, es sei denn dass diese Zuordnung eine größere Anzahl von Teilnehmern erfassen würde.

Use Case Internetzugangsdienste, Indikator IP-Adresse

Anforderung: Auskunft gemäß §76a (2) Z 1 StPO nach der IP Adresse 192.0.2.6 zum Zeitpunkt 13.1.2010, 01:00:00 Uhr.

Dateiname: 200001.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF
"200001","IP","192.0.2.6","KENN","45672000","Max","Mustermann"
,
"2343 Wr. Neustadt, Landstrasse 27" CRLF
```

Abfrage nach § 76a (2) Z 2 StPO

Anforderung: Auskunft über die bei Verwendung von E-Mail Diensten dem Teilnehmer zugewiesene Teilnehmerkennung.

Use Case E-Mail Verkehrsdaten

Anforderung: Auskunft gemäß §76a (2) Z 2 StPO nach der E-Mail Adresse max@example.com

Bemerkung: Bei dieser Abfrage werden die aktuellen Daten übermittelt.

Dateiname: 200002.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Zeit","GesendetAbsender","GesendetAbsende
rIP_Adresse",
"GesendetEmpfaenger","EmpfangAbsender","EmpfangZiel","EmpfangI
P_Adresse" CRLF
"200002","MAIL","max@example.com","NR","4319918767",#,#,#,#,#,
#,# CRLF
```

Abfrage nach § 76a (2) Z 3 StPO

Anforderung: Auskunft über Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war.

Diese Anfrage entspricht zunächst jener nach Kapitel 5.5., wobei historische Daten erhoben werden. Im zweiten Schritt erfolgt die Zuordnung zu den damals gültigen Stammdaten.

Abfrage nach § 76a (2) Z 4 StPO

Anforderung: Auskunft über die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders einer E-Mail.

Use Case E-Mail Verkehrsdaten

Anforderung: Auskunft gemäß §76a (2) Z 4 StPO nach der E-Mail Adresse max@example.com

Dateiname: 200003.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Zeit","GesendetAbsender","GesendetAbsende
rIP_Adresse",
"GesendetEmpfaenger","EmpfangAbsender","EmpfangZiel","EmpfangI
P_Adresse" CRLF
```

Empfangene E-Mail:

```
"200003","MAIL","max@example.com","NR","4319918767",
```

```
"2010-01-
12T21:23:12+01",#,#,#,"mona@example.com","max@example.com",
"192.0.2.10" CRLF
```

Auskunft nach § 53 (3a) Z 2 SPG

Anforderung: Auskunft über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung.
Bemerkung: Die Schnittstellendefinition gemäß § 94 (4) TKG richtet sich schon aufgrund der Normenadressaten ausschließlich an Anbieter im Sinne des TKG, nicht jedoch an Anbieter von "Diensten der Informationsgesellschaft" im Sinne des § 3 Z 2 E-Commerce-Gesetz, auf den § 53 (3a) Z 2 SPG ebenfalls verweist. In dieser Schnittstellendefinition sind daher nur jene Use-Cases erfasst, welche einen Anbieter im Sinne des TKG überhaupt betreffen können. Im Hinblick auf den Regelungsgehalt des § 53 (3a) Z 2 SPG (siehe oben) kann dies nur Anbieter von E-Mail Diensten betreffen, während beispielsweise Logfiles zu Webshops, Foren, Chatrooms, etc. sich ausschießlich nach dem ECG richten und daher nicht von dieser Schnittstellendefinition erfasst sind. Die Übermittlung von Auskünften solcher Anbieter wird durch die gegenständlichen Rechtsänderungen nicht berührt.
Arbeitshypothese ist, dass die Nachricht durch E-Mail Adresse von Sender und Empfänger sowie den Zeitpunkt der Übermittlung identifiziert wird. Dementsprechend kann der Use Case E-Mail Verkehrsdaten für Sende- oder Empfangsadresse herangezogen werden. Im folgenden Beispiel wird die Sendeadresse ausgewertet. Die IP-Adresse bezieht sich auf den Sender. In gleicher Weise kann eine Abfrage der Empfänger E-Mail Adresse erfolgen, welche dann die IP-Adresse des Empfängers liefert.

Use Case E-Mail Verkehrsdaten

Anforderung: Auskunft nach § 53 (3a) Z 2 SPG zur E-Mail Sendeadresse max@example.com und Empfangsadresse Mona@example.com, Zeitpunkt
Dateiname: 300001.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Zeit","GesendetAbsender","GesendetAbsende
rIP_Adresse",
"GesendetEmpfaenger","EmpfangAbsender","EmpfangZiel","EmpfangI
P_Adresse" CRLF
```

Gesendete E-Mail:

```
"300001","MAIL","max@example.com","NR","4319918767",
"2010-01-12T21:23:00+01","max@example.com","192.0.2.20",
"mona@example.com",#,#,# CRLF
```

Abfrage nach § 53 (3a) Z 3 SPG

Anforderung: Auskunft über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war.

Use Case Internetzugangsdienste, Indikator IP-Adresse

Anforderung: Auskunft nach § 53 (3a) Z 3 SPG zur IP Adresse 112.64.33.121 zum Zeitpunkt 13.1.2010, 01:00:00 Uhr.
Bemerkung: Die Teilnehmerkennung wird für diese Abfrage nicht übermittelt.
Dateiname: 300002.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF
"300002","IP","112.64.33.121",#,#,"Max","Mustermann",
"1234 Stockerau, Landstrasse 27" CRLF
```

Anfrage nach § 53 (3a) Z 4 SPG

Anforderung: Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer.

Use Case Öffentliche Telefondienste, Indikator Festnetznummer bzw. MSISDN

Bemerkung: Für diese Auswertung sind zunächst die Verkehrsdaten der vorgegebenen passiven Teilnehmernummer abzufragen. Dabei werden sich u.U. mehrere A-Rufnummern ergeben, weil die Anfrage lediglich unter Angabe eines möglichst genauen Zeitraumes zu erfolgen hat, der gemäß Erlass des BMI maximal eine Stunde betragen darf. Je stärker dieser Zeitraum bei der Anfrage eingeschränkt wird, desto zielgenauer kann die Auskunft erfolgen und damit der Verfahrensaufwand reduziert werden. Die Ermittlung der zugehörigen Stammdaten kann allerdings nur durch den jeweiligen Netzbetreiber erfolgen. Daher ist für diese Auswertung u.U. eine zweistufige Vorgangsweise erforderlich.

Anforderung: Auskunft gemäß § 53 (3a) Z 4 SPG zur Zielrufnummer Wien 991 5432 zwischen 12.1.2010, 23:00 und 24:00 Uhr.

Dateiname: 300003.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","Indik
atorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Ze
it","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI
",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anruf
umleitung" CRLF
"300003","ZIEL","4319915432",#,#,#,#,#,#,#,#,#,
"2010-01-12T21:23:30+01","22","T","A","4319914534",#,#,#,#,#,#
CRLF
```

Bemerkung: In diesem Beispiel wird eine Telefonverbindung zu dieser Zielrufnummer von der Wiener Rufnummer 991 4534 aufgezeichnet. Zu dieser Rufnummer sind keine Stammdaten enthalten, da sich diese in einem Fremdnetz befindet.

Zur Ermittlung der Stammdaten muss eine Anfrage an den Betreiber gestellt werden, in dessen Netz die Rufnummern 991 4534 angeschaltet ist.

Anfrage nach § 53 (3b) SPG

Anforderung: Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung.

Use Case Öffentliche Telefondienste, Indikator MSISDN

Anforderung: Auskunft nach § 53 (3b) SPG zur MSISDN 0665 98 75634 zur Ermittlung des aktuellen Aufenthaltsorts

Bemerkung: Die Beauskunftung wird im Regelfall wegen Gefahr im Verzug formlos telefonisch erfolgen. Die Anfrage muss aber über die DLS nachgereicht werden.

Dateiname: 300004.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","Indik
atorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Ze
it","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI
",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anruf
umleitung" CRLF
"300004","MSIS","436659875634",#,"232031234567890",#,#,#,#,"T-
Mobile",
"87543","16.151715/45.758972",#,#,#,#,#,#,#,#,#,#,# CRLF
```

Vorblatt

Probleme und Ziele:

Mit § 94 Abs. 4 Telekommunikationsgesetz 2003 (TKG 2003) wird der Bundesminister für Verkehr, Innovation und Technologie ermächtigt, die näheren Bestimmungen zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsslung, zur Speicherung und Übermittlung der Daten sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle festzusetzen.

Mit § 102c TKG 2003 wird der Bundesminister für Verkehr, Innovation und Technologie ermächtigt, eine nähere Beschreibung des Sorgfaltsmaßstabs zur Gewährleistung der Datensicherheit festschreiben.

Von diesen beiden Verordnungsermächtigungen soll nun Gebrauch gemacht und mit der vorliegenden Verordnung die Bestimmungen festgesetzt werden, die einerseits als Grundlage zur Einrichtung einer Durchlaufstelle (DLS) dienen und deren Aufgaben und deren Funktionsweise beschreiben sowie andererseits den von Anbietern von Kommunikationsdiensten einzuhaltenden Sicherheitsmaßstab regeln.

Die Grundlagen für diese Verordnung bilden die Studie zur „Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung“, welche das Ludwig Boltzmann Institut für Menschenrechte (BIM) im Auftrag des BMVIT ausgearbeitet hat, sowie die Diskussionen der insgesamt 6 Round Table Veranstaltungen des BIM im ersten Halbjahr 2011 zur Entwicklung der Schnittstellenbeschreibung und eines sicheren Systems der Datenübermittlung.

Inhalt:

- Konkretisierung der Datensicherheitsmaßnahmen innerhalb des Betriebs von Anbietern
- Konkretisierung der Datensicherheitsmaßnahmen bei Übermittlung der Daten
- Darstellung der Grundstruktur und der Funktionen der Durchlaufstelle (DLS)
- Einrichtung und Betrieb der DLS
- Auditierung der DLS-Funktionen
- Einbindung in den Portalverbund
- Erstellung der und Zugang zur Zugriffsstatistik

Alternativen:

Keine.

Auswirkungen des Regelungsvorhabens:

– Finanzielle Auswirkungen:

Für die Erfassung der Kosten der DLS ist zunächst von Bedeutung, dass die DLS einen Teil der Umsetzung der Richtlinie zur Vorratsdatenspeicherung 2006/24/EG darstellt, weil die besonderen Anforderungen an die Datensicherheit ihre Grundlage in Art 7 Lit. c) dieser Richtlinie haben: „in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist.“ Denselben Standard auf die Abwicklung aller Datenauskünfte (auch Daten, die zu Verrechnungszwecken vorhanden sind, nicht nur „Vorratsdaten“) anzuwenden ist dabei nicht nur konsequent sondern auch aus rein praktischen Gründen notwendig. Viele Auskünfte werden nämlich künftig wohl „gemischte“ Datensätze enthalten, also in derselben Auskunft Vorratsdaten und Betriebsdaten. Diese Annahme ist deshalb wesentlich, weil es bzgl. der Vorratsdatenspeicherung in der Regierungsvorlage zum TKG 2003 klare Regeln zur Kostentragung gibt. Der initiale Investitionsaufwand (Investitionskosten) zur Schaffung der für die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung notwendigen Infrastruktur wird für die gesamte österreichische Telekommunikationsbranche geschätzte 15 Millionen Euro betragen und wird gem. § 94 Abs. 1 TKG 2003 zu 80% vom Bund ersetzt. Dafür ist ein Aufteilungsschlüssel zwischen den Ministerien (BMVIT, BMI und BMJ) vorgesehen. Bei der Verabschiedung der gemeinsamen Regierungsvorlage zur TKG-Novelle wurde nämlich eine Vereinbarung zur Aufteilung dieser Kosten auf die Ministerien BMI (34%), BMJ (Fixbetrag von Euro 360.000,--) und BMVIT (63%) getroffen.

Die Einrichtungskosten der DLS für die Umsetzung der Vorratsdatenspeicherung fallen zwar direkt beim Bund an, stehen aber in unmittelbarem Zusammenhang zu den Investitionskosten der Anbieter, da im Gegensatz zu einer dezentralen S/MIME, wo die Kosten direkt bei den Anbietern anfielen und dem Investitionskostenersatz nach § 94 abs. 1 TKG 2003 unterlägen, wesentlich günstiger sind.

Die Bundesrechenzentrum GmbH (BRZ) schätzt die Investitionskosten auf knapp unter 500.000,- Euro, die monatlichen Betriebskosten wurden mit 7.000,- Euro beziffert. Die Schätzung ist vorsichtig angelegt, damit nicht zu befürchten ist, dass sich im Falle einer tatsächlichen Umsetzung die Kosten dann als deutlich höher erweisen.

Dieser Kostenschätzung liegen folgende Annahmen zugrunde:

Authentifizierung mittels qualifizierter Signatur

Nutzung vorhandener Infrastruktur des BRZ (bestehende Serversysteme)

Maximale Größe der zu übermittelnden Daten 15 MB

Die Schätzung enthält ein Portal für Netzbetreiber ähnlich dem Portalverbund.

Die Funktion eines Help-desk ist nicht enthalten.

Aufwendungen für erhöhte Sicherheit sind in der Kostenschätzung nicht enthalten.

Die Kosten für die Auditierung der tatsächlichen Umsetzung durch die BRZ, die durch einen Dienstleister erfolgen muss, werden auf 49.500,- Euro geschätzt.

Die durch die Einrichtung der DLS verursachten Investitionskosten für den Bund in Höhe von rund 500.000,-- Euro, die beispielsweise bei der verschlüsselten Übermittlung per E-Mail (ursprünglich im Begutachtungsentwurf zur TKG-Novelle vorgesehenes „S/MIME Konzept“) nicht anfallen, sind in die Investitionskosten nach § 94 Abs. 1 TKG 2003 einzuberechnen. Die Einrechnung dieser Kosten in die zu 80% zu erstattendenden Investitionskosten der Anbieter ist gerechtfertigt, da bei der Implementierung eines dezentralen S/MIME Konzepts die Anbieter (nach Angaben der RTR sind dzt. ca 200 Anbieter gemäß § 102a TKG 2003 speicherpflichtig) und mindestens 15 anfrageberechtigte Stellen auf Seiten der Sicherheitsbehörden dezentral sichere Wege zur Datenübermittlung und zur Authentifizierung schaffen müssten. Das würde erfordern, dass die technische Implementierung mit allen Anbietern einzeln definiert und implementiert werden müsste. Allein der dezentrale Austausch der Sicherheits-Zertifikate würde dabei schon einen beträchtlichen Aufwand verursachen. Demgegenüber muss die Spezifikation zur DLS nur einmal ausgearbeitet werden (unter Beteiligung der Telekom Branche, die dabei teilweise auch über die Interessenvertretungen erfolgt und nicht für alle - vor allem kleinere - Anbieter unmittelbar Aufwand verursacht). Die zentrale Architektur und vor allem die zentrale Hinterlegung der „publickeys“ vereinfachen diese Prozesse enorm. Der einzelne Anbieter benötigt für die Abwicklung nur noch einen herkömmlichen Internet-Browser für eine sicher Verbindung (per https) zur Durchlaufstelle.

Der Entwicklungsaufwand für die Spezifikation der Schnittstelle stellt bei den Anbietern Investitionskosten dar, die im Sinne des § 94 Abs. 1 TKG dem Investitionskostenersatz unterliegen. Der Aufwand für die Spezifikation der Schnittstelle eines dezentralen S/MIME Konzepts wäre deutlich höher als jener einer zentralen DLS. Unter der Annahme, dass der Aufwand für die Spezifikation eines dezentralen Konzepts auf Seiten aller Anbieter insgesamt Kosten in Höhe von 625.000,- Euro verursacht (wovon 80% - also 500.000,- Euro - vom Bund zu erstatten wären), ist die DLS auch vom Investitionskostenaufwand her günstiger als eine verschlüsselte Übermittlung per E-Mail. Bei 200 Anbietern wird diese Schwelle erreicht, wenn im Durchschnitt Mehrkosten in Höhe von 3.125,- Euro pro Anbieter entstehen. Bei marktüblichen Stundensätzen für qualifizierte IT Techniker würde diese Schwelle wohl erheblich überschritten werden, weil ein durchschnittlicher Mehraufwand von zwei bis drei Arbeitstagen pro Unternehmen selbst bei vorsichtiger Schätzung von allen Beteiligten als realistisch bezeichnet wurde.

Die Implementierungskosten der DLS sind sachlich von dem mit etwa 15.000.000 Euro bezifferten Budgetvolumen erfasst, die der Bund für die Investitionskosten zur Umsetzung der Vorratsdatenspeicherung veranschlagt hat. Die Implementierung der DLS bedeutet auf Seiten der Sicherheitsbehörden eine Effizienzerhöhung und damit eine deutliche Kostenersparnis. Der geringere Aufwand für die Spezifikation der Schnittstelle bei der zentralen DLS Lösung wird dabei vor allem beim Innenministerium / Bundeskriminalamt spürbar sein, wo die faktische Abwicklung der Auskunftsvorgänge implementiert werden muss. Dementsprechend ist - in der Relation der Investitionskosten der DLS zu den Investitionskosten der Anbieter - auch hier eine Kostenteilung zwischen den Ressorts sachgerecht.

Am stärksten spürbar sein wird die Erleichterung für die Sicherheitsbehörden im operativen Betrieb. Durch stärkere Automatisierung und die zentrale Kommunikation über die DLS wird bei den Auskunftsbegehren von Seiten des Bundeskriminalamts eine Aufwandsersparnis erwartet. Die größte Aufwandsreduzierung besteht vor allem darin, dass im Vergleich zum dezentralen S/MIMe Konzept die laufende Erneuerung der Sicherheitszertifikate zentral erfolgt und damit massiv erleichtert wird. Die Erfahrung aus der Europol Kooperation zeigt, dass dies bei einer dezentralen sicheren Kommunikation

zwischen vielen Stellen ein enormer Aufwands- und damit Kostensteigerungsfaktor ist. Eine unverbindliche Einschätzung seitens der IT-Abteilung des BMI geht davon aus, dass die „S/MIME Variante“ hier einen Mehraufwand im Ausmaß einer vollen Planstelle bedeuten würde. Stellt man dem die geschätzten laufenden monatlichen Kosten der DLS in Höhe von rund 7.000,- Euro entgegen, zeigt sich auch für den operativen Betrieb die DLS als die kostengünstigere Variante.

Die Bedeckung der laufenden Kosten (Betriebskosten) der DLS erfolgt aus vorhandenen Budgetmitteln der beteiligten Ressorts. Die Aufteilung der laufenden Kosten bleibt einer interministeriellen Vereinbarung vorbehalten.

– Wirtschaftspolitische Auswirkungen:

– – Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Keine.

– – Auswirkungen auf die VerwaltungskostenfürBürger/innen und für Unternehmen:

Für Bürger/innen fallen keine Kosten an.

Die sich durch die Einführung der Verpflichtung zur Vorratsdatenspeicherung für Unternehmen ergebenden Kosten wurden bereits im Vorblatt zur Novelle des TKG 2003, BGBl. I Nr. 27/2011 (1074 der Beilagen XXIV. GP) dargelegt. Es darf hierauf verwiesen werden.

– Auswirkungen in umweltpolitischer Hinsicht, insbesondere Klimaverträglichkeit:

Es sind keine umweltpolitischen Auswirkungen zu erwarten.

Das Regelungsvorhaben ist nicht klimarelevant.

– Auswirkungen in konsumentenschutzpolitischer sowie sozialer Hinsicht:

Es sind weder konsumentenschutzpolitische noch soziale Auswirkungen zu erwarten.

– Geschlechtsspezifische Auswirkungen:

Genderspezifische Auswirkungen sind nach dem Inhalt des vorliegenden Entwurfes nicht zu erwarten, da die Normadressaten ausschließlich Unternehmen und Behörden sind.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Gegeben. Der Entwurf dient stellenweise der Umsetzung von Gemeinschaftsrecht. Die darüber hinaus vorgesehenen Regelungen fallen nicht in den Anwendungsbereich des Rechts der Europäischen Union.