Gesamte Rechtsvorschrift für Datensicherheitsverordnung, Fassung vom 05.02.2026

Langtitel

Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO)
StF: BGBl. II Nr. 402/2011

Änderung

BGBl. II Nr. 228/2016

Präambel/Promulgationsklausel

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. 102/2011, wird, hinsichtlich der §§ 1 bis 4 und 8 bis 25 im Einvernehmen mit dem Bundesminister für Inneres und dem Bundesminister für Justiz, verordnet:

Text

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. 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. 67/2011, und
4. bei der Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten.

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.

(2) Wenn eine Auskunft Vorratsdaten enthält, hat der Anbieter diesen Umstand als Zusatzinformation 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.

(4) Enthält eine Auskunft Vorratsdaten, die gemäß Abs. 3 zugleich als Betriebsdaten gespeichert sind, hat der Anbieter diesen Umstand als Zusatzinformation zu übermitteln.

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 oder Betriebsdaten im Fall einer Anordnung der Staatsanwaltschaft gemäß § 135 Abs. 2a StPO 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 § 17 Abs. 1) sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft (Zustellung der Antwort in das Postfach der Behörde in der Durchlaufstelle gemäß § 17 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. 1 Z 1) und als Vorratsdaten gemäß § 2 Abs. 1 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 Abs. 3a und 3b 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, ansonsten den Hinweis, dass nur Betriebsdaten verwendet werden.

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 der Bundesminister 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 und des § 99 Abs. 3a Finanzstrafgesetz-FinStrG, BGBl. Nr. 129/1958 in der Fassung BGBl. I Nr. 118/2015. 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 § 4 Z 5 des Datenschutzgesetzes 2000 (DSG 2000), BGBl. I Nr. 165/1999 in der Fassung BGBl. I Nr. 133/2009, 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 und der Betrieb der Durchlaufstelle sowie die Zertifikatsverwaltung und die Datensicherheit liegen in der Verantwortung des Bundesministers 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 und des § 99 Abs. 3a FinStrG 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 § 22 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, Version 2.1.0 vom 8. Februar 2008, abrufbar unter „http://reference.e-government.gv.at/uploads/media/SecClass_2-1-0_2007-12-14.pdf“, der Portalverbundvereinbarung, Version 1.0 vom 21. November 2002, abrufbar unter „http://reference.e-government.gv.at/uploads/media/pvv1.0-21112002.pdf“, entspricht.

Zugangsberechtigte Behörden

§ 14. (1) Der Bundesminister für Inneres, der Bundesminister für Justiz sowie der Bundesminister für Finanzen 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 den Bundesminister für Inneres, den Bundesminister für Justiz sowie den Bundesminister für Finanzen der Bundesrechenzentrum GmbH für die Veranlassung der entsprechenden Änderungen in der Durchlaufstelle bekannt zu geben.

(3) Für die Datenschutzkommission, den Bundesminister 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, Version 1.3 vom 24. Juli 2003, abrufbar unter „http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=21832“ 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 dem Anbieter vollautomatisch durch die Durchlaufstelle eine Unique-ID vergeben.

(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 § 11 Abs. 1 Z 5 oder 7 Polizeiliches Staatsschutzgesetz – PStSG, BGBl. I Nr. 5/2016, nach § 76a StPO, nach § 135 Abs. 2 StPO, nach § 99 Abs. 3a FinStrG 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 5 und 8 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 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 20023/58/EG, ABl. Nr. L 105 vom 13. April 2006, S 54, 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 5 und 8 hat der Anbieter gemeinsam mit der Beantwortung des Auskunftsbegehrens an die Durchlaufstelle zu übermitteln.

(3) Zugang zur Statistik der Durchlaufstelle erhalten gemäß § 102c Abs. 4 TKG 2003 der Bundesminister 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.

Anlage

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

(Anm.: Anlage als PDF dokumentiert)

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.

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	#	
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.

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

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 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 Kapitel 1.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt	siehe Kapitel

	oder enthält optional die Zielrufnummer der Anrufumleitung	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:

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

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

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