

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2011**Ausgegeben am 5. Dezember 2011****Teil II**

402. Verordnung: Datensicherheitsverordnung TKG-DSVO

402. Verordnung der Bundesministerin 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. 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:

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. 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 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 sowie der Bundesminister 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 den Bundesminister für Inneres sowie den Bundesminister für Justiz 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 Protokoll Daten 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 Abholung 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 Spezifikation 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 2002/58/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.

Bures

