

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2011

Ausgegeben am 18. Mai 2011

Teil I

27. Bundesgesetz: **Änderung des Telekommunikationsgesetzes 2003 – TKG 2003**
(NR: GP XXIV RV 1074 AB 1157 S. 102. BR: AB 8493 S. 796.)
[CELEX-Nr.: 32006L0024]

27. Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird

Der Nationalrat hat beschlossen:

Das Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I Nr. 70/2003, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 50/2010, wird wie folgt geändert:

1. In § 1 Abs. 4 wird der Punkt nach Z 5 durch einen Strichpunkt ersetzt und folgende Z 6 angefügt:

„6. 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.“

2. In § 78 Abs. 2 wird nach dem Ausdruck „Datenschutzgesetzes 2000“ der Klammerausdruck „(DSG 2000)“ eingefügt.

3. In § 87 Abs. 2 wird das Wort „Sicherheitspolizeigesetz“ durch die Wortfolge „des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991,“ ersetzt; weiters wird der Ausdruck „StPO“ durch die Wortfolge „der Strafprozessordnung 1975 (StPO), BGBl. Nr. 631,“ ersetzt.

4. § 90 Abs. 6 lautet:

„(6) Anbieter von Kommunikationsdiensten sind 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.“

5. In § 90 werden nach Abs. 6 nachfolgende Abs. 7 und 8 angefügt:

(7) Anbieter von Kommunikationsdiensten sind 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.

(8) Anbieter von Mobilfunknetzen haben Aufzeichnungen über den geografischen Standort der zum Betrieb ihres Dienstes eingesetzten Funkzellen zu führen, sodass jederzeit die richtige Zuordnung einer Standortkennung (Cell-ID) zum tatsächlichen geografischen Standort unter Angabe von Geo-Koordinaten für jeden Zeitpunkt innerhalb eines sechs Monate zurückliegenden Zeitraums gewährleistet ist.“

6. In § 92 Abs. 2 entfällt der Ausdruck „(StPO), BGBl. Nr. 631/1975,“.

7. In § 92 Abs. 3 werden nach Z 2 folgende Z 2a und 2b eingefügt:

„2a. „Teilnehmerkennung“ jene Kennung, welche die eindeutige Zuordnung eines Kommunikationsvorgangs zu einem Teilnehmer ermöglicht;

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

8. § 92 Abs. 3 Z 3 lit. a bis c lauten:

„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:

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

b) akademischer Grad bei natürlichen Personen,

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

9. In § 92 Abs. 3 werden nach Z 6 nachfolgende Z 6a und 6b eingefügt:

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

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

10. § 92 Abs. 3 Z 8 lautet:

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

11. In § 92 Abs. 3 wird nach Z 8 nachfolgende Z 8a eingefügt:

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

12. Der Punkt nach § 92 Abs. 3 Z 10 wird durch einen Strichpunkt ersetzt und folgende Z 11 bis 16 angefügt:

- „11. „elektronisches Postfach“ ein elektronisches Ablagesystem, das einem Teilnehmer eines E-Mail-Dienstes zugeordnet ist;
12. „E-Mail“ elektronische Post, die über das Internet auf Basis des „Simple Mail Transfer Protocol“ (SMTP) versendet wird;
13. „Internet-Telefondienst“ einen öffentlichen Telefondienst im Sinne des § 3 Z 16, der auf paketvermittelter Nachrichtenübertragung über das Internet-Protokoll basiert;
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;
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 Protocol“ (SMTP) umfasst;
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.“

13. § 93 Abs. 3 lautet:

„(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung, der Überwachung von Nachrichten und der Auskunft über Daten einer Nachrichtenübermittlung einschließlich Vorratsdaten sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.“

14. § 93 wird folgender Abs. 5 angefügt:

„(5) Das Redaktionsgeheimnis (§ 31 Mediengesetz) sowie sonstige, in anderen Bundesgesetzen normierte Geheimhaltungsverpflichtungen sind nach Maßgabe des Schutzes der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen sowie das Verbot deren Umgehung gemäß §§ 144 und 157 Abs. 2 StPO zu beachten. Den Anbieter trifft keine entsprechende Prüfpflicht.“

15. § 94 samt Überschrift lautet:

„Technische Einrichtungen

§ 94. (1) Der Anbieter ist nach Maßgabe der gemäß Abs. 3 und 4 erlassenen Verordnungen verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten sowie zur Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten nach den Bestimmungen der StPO erforderlich sind. Für die Bereitstellung sind dem Anbieter 80% der Kosten (Personal- und Sachaufwendungen), die er aufwenden musste, um die gemäß den Abs. 3 und 4 erlassenen Verordnungen erforderlichen Funktionen in seinen Anlagen einzurichten, zu ersetzen. Der Bundesminister für Verkehr, Innovation und Technologie hat im Einvernehmen mit dem Bundesminister für Inneres, dem Bundesminister für Justiz und dem Bundesminister für Finanzen durch Verordnung die Bemessungsgrundlage für diesen Prozentsatz sowie die Modalitäten für die Geltendmachung dieses Ersatzanspruches festzusetzen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, sowie auf die Einfachheit und Kostengünstigkeit des Verfahrens Bedacht zu nehmen.

(2) Der Anbieter ist verpflichtet, an der Überwachung von Nachrichten sowie der Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten nach den Bestimmungen der StPO im erforderlichen Ausmaß mitzuwirken. Der Bundesminister für Justiz hat im Einvernehmen mit dem Bundesminister für Verkehr, Innovation und Technologie und dem Bundesminister für Finanzen durch

Verordnung einen angemessenen Kostenersatz vorzusehen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, sowie der öffentlichen Aufgabe der Rechtspflege Bedacht zu nehmen.

(3) Durch Verordnung kann der Bundesminister für Verkehr, Innovation und Technologie im Einvernehmen mit den Bundesministern für Inneres und für Justiz dem jeweiligen Stand der Technik entsprechend die näheren Bestimmungen für die Gestaltung der technischen Einrichtungen zur Gewährleistung der Überwachung von Nachrichten nach den Bestimmungen der StPO und zum Schutz der zu übermittelnden Daten gegen die unbefugte Kenntnisnahme oder Verwendung durch Dritte festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten.

(4) 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. Ausgenommen davon ist die Übermittlung von Daten in den Fällen des § 98, von Daten in den Fällen von § 99 Abs. 5 Z 3 und 4 bei Gefahr in Verzug, von Standortdaten in den Fällen der Feststellung des aktuellen Standortes gemäß §§ 134 ff StPO sowie die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten. Durch Verordnung kann der Bundesminister für Verkehr, Innovation und Technologie im Einvernehmen mit den Bundesministern für Inneres und für Justiz die näheren Bestimmungen zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsselung, zur Speicherung und Übermittlung der Daten sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten."

16. § 97 Abs. 1 lautet:

„(1) Stammdaten dürfen unbeschadet der §§ 90 Abs. 6 und 7 sowie 96 Abs. 1 und 2 von Anbietern nur für folgende Zwecke ermittelt und verwendet werden:

1. Abschluss, Durchführung, Änderung oder Beendigung des Vertrages mit dem Teilnehmer;
2. Verrechnung der Entgelte;
3. Erstellung von Teilnehmerverzeichnissen, gemäß § 18 und
4. Erteilung von Auskünften an Notrufträger.“

17. Der bisherige § 98 wird als Abs. 1 bezeichnet und folgender Abs. 2 angefügt:

„(2) Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung des gefährdeten Menschen verarbeitet werden, auch wenn hierfür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist. Der Anbieter hat den betroffenen Teilnehmer über eine Auskunft über Standortdaten nach dieser Ziffer frühestens nach 48 Stunden, jedoch spätestens nach 30 Tagen grundsätzlich durch Versand einer Kurzmitteilung (SMS), wenn dies nicht möglich ist schriftlich, zu informieren. Diese Information hat zu enthalten:

- a) die Rechtsgrundlage,
- b) die betroffene Daten,
- c) das Datum und die Uhrzeit der Abfrage,
- d) Angabe der Stelle, von der die Standortfeststellung in Auftrag gegeben wurde, sowie eine entsprechende Kontaktinformation.“

18. § 99 Abs. 1 lautet:

„(1) Verkehrsdaten dürfen außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Die Zulässigkeit der weiteren Verwendung von Verkehrsdaten, die nach Abs. 5 übermittelt werden, richtet sich nach den Vorschriften der StPO sowie des SPG.“

19. § 99 Abs. 4 lautet:

„(4) Dem Anbieter ist es außer in den in diesem Gesetz besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Anbieter die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden.“

20. In § 99 wird nach Abs. 4 folgender Abs. 5 angefügt:

„(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist zulässig zur Auskunft über

1. Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO;
2. Zugangsdaten, auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1, Abs. 3 Z 6 lit. a und b oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden, an Gerichte und Staatsanwaltschaften nach Maßgabe des § 76a Abs. 2 StPO.
3. Verkehrsdaten und Stammdaten, wenn hiefür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a und 3b SPG. Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung verarbeitet werden, auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist;
4. Zugangsdaten, auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2,3 und 5 längstens drei Monate vor der Anfrage gespeichert wurden, an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 3 SPG.“

21. Dem § 102 Abs. 3 wird folgender Satz angefügt:

„Unbeschadet des § 93 Abs. 3 ist die Ermittlung und Verwendung von Standortdaten, die nicht im Zusammenhang mit einem Kommunikationsvorgang stehen, zu Auskunftszwecken unzulässig.“

22. Nach § 102 werden folgende §§ 102a, 102b und 102c samt Überschriften eingefügt:

„Vorratsdaten

§ 102a. (1) Über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus haben Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt.

(2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;
2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internet-Zugangsdienst unter Angabe der zugrundeliegenden Zeitzone;
3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
4. die eindeutige Kennung des Anschlusses, über den der Internet-Zugang erfolgt ist.

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

1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;
2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;
3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;
4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;
5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste).
6. Bei Mobilfunknetzen zudem
 - a) der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;
 - b) der internationalen Mobilfunkgeräteerkennung (IMEI) des anrufenden und des angerufenen Anschlusses;
 - c) 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;
 - d) der Standortkennung (Cell-ID) bei Beginn einer Verbindung.

(4) Anbietern von E-Mail-Diensten obliegt die Speicherung folgender Daten:

1. die einem Teilnehmer zugewiesene Teilnehmerkennung;
2. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war;
3. 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;
4. 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;
5. bei An- und Abmeldung beim E-Mail-Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrunde liegenden Zeitzone.

(5) Die Speicherpflicht nach Abs. 1 besteht nur für jene Daten gemäß Abs. 2 bis 4, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden. Im Zusammenhang mit erfolglosen Anrufversuchen besteht die Speicherpflicht nach Abs. 1 nur, soweit diese Daten im Zuge der Bereitstellung des betreffenden Kommunikationsdienstes erzeugt oder verarbeitet und gespeichert oder protokolliert werden.

(6) Die Speicherpflicht nach Abs. 1 besteht nicht für solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 34 KommAustriaG unterliegen.

(7) Der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(8) Die nach Abs. 1 zu speichernden Daten sind nach Ablauf der Speicherfrist unbeschadet des § 99 Abs. 2 unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen. Die Erteilung einer Auskunft nach Ablauf der Speicherfrist ist unzulässig.

(9) Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden, richten sich die Ansprüche auf Information oder Auskunft über diese Datenverwendung ausschließlich nach den Bestimmungen der StPO.

Auskunft über Vorratsdaten

§ 102b. (1) Eine Auskunft über Vorratsdaten ist ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig.

(2) Die nach § 102a zu speichernden Daten sind so zu speichern, dass sie unverzüglich an die nach den Bestimmungen der StPO und nach dem dort vorgesehenen Verfahren für die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können.

(3) Die Übermittlung der Daten hat in angemessen geschützter Form nach Maßgabe des § 94 Abs. 4 zu erfolgen.

Datensicherheit, Protokollierung und Statistik

§ 102c. (1) Die Speicherung der Vorratsdaten hat so zu erfolgen, dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist. Die Daten sind durch geeignete technische und organisatorische Maßnahmen vor unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen. Ebenso ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den Vorratsdaten ausschließlich dazu ermächtigten Personen unter Einhaltung des Vier-Augen-Prinzips vorbehalten ist. Die Protokolldaten sind drei Jahre ab Ende der Speicherfrist für das betreffende Vorratsdatum zu speichern. Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für die Datenschutzkontrolle gemäß § 30 DSGVO zuständigen Datenschutzkommission. Eine nähere Beschreibung des Sorgfaltsmaßstabs zur Gewährleistung der Datensicherheit kann der Bundesminister für Verkehr, Innovation und Technologie per Verordnung festschreiben.

(2) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben zu gewährleisten, dass jeder Zugriff auf Vorratsdaten sowie jede Anfrage und jede Auskunft über Vorratsdaten nach § 102b reversionssicher protokolliert wird. Diese 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 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft,
4. die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung,
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt sowie
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben.

(3) Die Speicherung der Protokolldaten hat so zu erfolgen, dass deren Unterscheidung von Vorratsdaten sowie von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherter Daten möglich ist.

(4) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben

1. für Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit die Protokolldaten gemäß Abs. 2 an die Datenschutzkommission und den Datenschutzrat sowie
2. zum Zweck der Berichterstattung an die Europäische Kommission und an den Nationalrat die Protokolldaten gemäß Abs. 2 Z 2 bis 4 an den Bundesminister für Justiz zu übermitteln.

(5) Die Übermittlung der Protokolldaten hat auf schriftliches Ersuchen der Datenschutzkommission bzw. des Bundesministers für Justiz zu erfolgen; die Übermittlung an den Bundesminister muss darüber hinaus jährlich bis zum 31. Jänner für das vorangegangene Kalenderjahr erfolgen.

(6) Über die Protokollierungspflichten nach Abs. 2 hinaus ist eine Speicherung der übermittelten Datensätze selbst unzulässig.“

23. § 103 Abs. 4 entfällt.

24. § 109 Abs. 3 Z 14 lautet:

„14. entgegen § 94 Abs. 2 nicht an der Überwachung von Nachrichten oder an der Auskunft über Daten einer Nachrichtenübermittlung im erforderlichen Ausmaß mitwirkt;“

25. § 109 Abs. 3 Z 17 lautet:

„17. entgegen § 98 nicht Auskünfte über Stammdaten oder Standortdaten erteilt oder die Teilnehmer nicht informiert;“

26. In § 109 Abs. 3 wird der Punkt nach Z 20 durch einen Strichpunkt ersetzt und folgende Z 21 bis 26 werden angefügt:

„21. entgegen § 99 Abs. 5 Auskunft über Verkehrsdaten erteilt oder Verkehrsdaten zu Auskunftszwecken verarbeitet;

22. entgegen § 102a Daten nicht speichert; die Strafbarkeit besteht nicht, wenn die hierfür erforderlichen Investitionskosten noch nicht aufgrund einer nach § 94 Abs. 1 erlassenen Verordnung abgegolten wurden;

23. entgegen § 102a Abs. 8 Daten nicht löscht;

24. entgegen § 102b Daten ohne Vorliegen einer gerichtlichen Bewilligung beauskunftet;

25. entgegen § 102b Daten in nicht verschlüsselter Form über ein Kommunikationsnetz übermittelt;

26. entgegen § 102c nicht protokolliert oder die notwendigen Auskünfte erteilt.“

27. § 109 Abs. 4 Z 7 lautet:

„7. wer nicht technische Einrichtungen im Sinn des § 94 Abs. 1 bereit stellt. Die Strafbarkeit besteht nicht, wenn die hierfür erforderlichen Investitionskosten noch nicht aufgrund einer nach § 94 Abs. 1 erlassenen Verordnung abgegolten wurden;“

28. Nach § 136 wird folgender § 136a samt Überschrift eingefügt:

„Sprachliche Gleichbehandlung

§ 136a. Sämtliche in diesem Bundesgesetz verwendeten Funktionsbezeichnungen und personenbezogene Ausdrücke sind geschlechtsneutral zu verstehen.“

29. § 137 wird folgender Abs. 4 angefügt:

„(4) §§ 94 Abs. 1 und 102a Abs. 1 in der Fassung des Bundesgesetzes BGBl. I Nr. 27/2011 treten am 1. April 2012 in Kraft.“

30. Das Inhaltsverzeichnis vor § 1 wird wie folgt geändert:

§§ 94, 102a, 102b, 102c und 136a lauten:

„§ 94 Technische Einrichtungen
§ 102a Vorratsdaten
§ 102b Auskunft über Vorratsdaten
§ 102c Datensicherheit, Protokollierung und Statistik
§ 136a Sprachliche Gleichbehandlung“

Fischer

Faymann