Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 102/2011

§/Artikel/Anlage
§ 90

Inkrafttretensdatum
22.11.2011

Text

Informationspflichten

§ 90. (1) Betreiber von Kommunikationsnetzen oder -diensten sowie Inhaber von Nutzungsrechten an Frequenzen oder Kommunikationsparametern, sind verpflichtet, dem Bundesminister für Verkehr, Innovation und Technologie und der Regulierungsbehörde auf schriftliches Verlangen die Auskünfte zu erteilen, die für den Vollzug dieses Gesetzes und der relevanten internationalen Vorschriften notwendig sind. Dies sind insbesondere

1. Auskünfte für die systematische oder einzelfallbezogene Überprüfung der Verpflichtungen, die sich aus diesem Bundesgesetz oder aus einer auf Grund dieses Bundesgesetzes erlassenen Verordnung oder eines Bescheides ergeben,
2. Auskünfte für die einzelfallbezogene Überprüfung der Verpflichtungen, wenn der Regulierungsbehörde eine Beschwerde vorliegt oder sie aus anderen Gründen eine Verletzung von Pflichten annimmt oder sie von sich aus Ermittlungen durchführt,
3. Auskünfte in Verfahren auf Zuteilung von Frequenzen oder Kommunikationsparametern,
4. Auskünfte für ein Verfahren gemäß § 36 bis 37a,
5. Auskünfte für die Veröffentlichung von Qualitäts- und Preisvergleichen für Dienste zum Nutzen der Konsumenten, sowie
6. Auskünfte über künftige Netz- oder Dienstentwicklungen, die sich auf die jeweils bestehenden Dienste auf Vorleistungsebene auswirken könnten.

Diese Informationen sind binnen der hiefür gesetzten Frist und nach dem Zeitplan und in den Einzelheiten vorzulegen, die verlangt werden. Informationen gemäß Z 3 dürfen von Unternehmen auch vor Aufnahme ihrer Tätigkeit verlangt werden. Die verlangten Informationen müssen in angemessenem Verhältnis zur Wahrnehmung der Aufgaben stehen. Das Verlangen ist zu begründen und dem Betroffenen mitzuteilen, für welchen konkreten Zweck die bereitgestellten Informationen benutzt werden sollen. Eine Verweigerung der Auskunftserteilung unter Berufung auf vertraglich vereinbarte Betriebs- und Geschäftsgeheimnisse ist nicht zulässig. § 125 bleibt davon unberührt.

(2) Für die Beobachtung und Überwachung der Markt- und Wettbewerbsentwicklung gemäß § 34 wird der Bundesminister für Verkehr, Innovation und Technologie ermächtigt, die Erstellung von Statistiken für den Bereich Kommunikation anzuordnen. Die Erstellung von Statistiken hat durch die Regulierungsbehörde zu erfolgen.

(3) Die Verordnung gemäß Abs. 2 hat neben der Anordnung von statistischen Erhebungen insbesondere zu enthalten:

1. die Erhebungsmasse;
2. statistische Einheiten;
3. die Art der statistischen Erhebung;
4. Erhebungsmerkmale;
5. Häufigkeit und Zeitabstände der Datenerhebung;
6. die Bestimmung des Personenkreises, der zur Auskunft verpflichtet ist;
7. ob und in welchem Umfang die Ergebnisse der statistischen Erhebungen zu veröffentlichen sind, wobei die Bestimmungen des § 19 Abs. 2 Bundesstatistikgesetz 2000, BGBl. I Nr. 163/1999, zu beachten sind.

(4) Die Weitergabe von Einzeldaten an die Bundesanstalt “Statistik Österreich” für Zwecke der Bundesstatistik ist zulässig.

(5) Die Erstellung von Statistiken hat unter sinngemäßer Anwendung der Bestimmungen des Bundesstatistikgesetzes 2000, BGBl. I Nr. 163/1999, zu erfolgen.

(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.

(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.

Kurztitel

Telekommunikationsgesetz 2003

Kundmachungsorgan

BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 102/2011

§/Artikel/Anlage

§ 92

Inkrafttretensdatum

22.11.2011

Text

12. Abschnitt
Kommunikationsgeheimnis, Datenschutz
Allgemeines

§ 92. (1) Die Bestimmungen dieses Abschnitts gelten für die Verarbeitung und Übermittlung von personenbezogenen Daten in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen. Soweit dieses Bundesgesetz nicht anderes bestimmt, sind auf die in diesem Bundesgesetz geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, anzuwenden.

(2) Die Bestimmungen der Strafprozessordnung bleiben durch die Bestimmungen dieses Abschnittes unberührt.

(3) In diesem Abschnitt bezeichnet unbeschadet des § 3 der Begriff

1. "Anbieter" Betreiber von öffentlichen Kommunikationsdiensten;
2. "Benutzer" eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;

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;

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 (Familienname 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),
   d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
   e) Information über Art und Inhalt des Vertragsverhältnisses,
   f) Bonität;

4. "Verkehrsdaten" Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

4a. "Zugangsdaten" jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind;

5. "Inhaltsdaten" die Inhalte übertragener Nachrichten (Z 7);

6. "Standortdaten" Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen sind Standortdaten die Adresse der Einrichtung;

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;

7. "Nachricht" jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

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

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

9. "Dienst mit Zusatznutzen" jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

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;

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;

17. "Verletzung des Schutzes personenbezogener Daten" jede Verletzung der Sicherheit, die auf versehentliche oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlicher Kommunikationsdienste in der Gemeinschaft verarbeitet werden.

Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 102/2011

§/Artikel/Anlage
§ 93

Inkrafttretensdatum
22.11.2011

Text

Kommunikationsgeheimnis

§ 93. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber eines öffentlichen Kommunikationsnetzes oder –dienstes und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(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.

(4) Werden mittels einer Funkanlage, einer Telekommunikationsendeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Telekommunikationsendeinrichtung oder den Anwender der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke verwertet werden. Aufgezeichnete Nachrichten sind zu löschen oder auf andere Art zu vernichten.

(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.

Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 27/2011

§/Artikel/Anlage
§ 94

Inkrafttretensdatum
01.04.2012

Text

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.

Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 102/2011

§/Artikel/Anlage
§ 95

Inkrafttretensdatum
21.02.2012

Text

Datensicherheitsmaßnahmen

§ 95. (1) Die Pflicht zur Erlassung von Datensicherheitsmaßnahmen im Sinne des § 14 des Datenschutzgesetzes 2000 im Zusammenhang mit der Erbringung eines öffentlichen Kommunikationsdienstes obliegt jedem Betreiber eines öffentlichen Kommunikationsdienstes jeweils für jeden von ihm erbrachten Dienst.

(2) Unbeschadet des Abs. 1 hat der Betreiber eines öffentlichen Kommunikationsdienstes in jenen Fällen, in denen ein besonderes Risiko der Verletzung der Vertraulichkeit besteht, die Teilnehmer über dieses Risiko und - wenn das Risiko außerhalb des Anwendungsbereichs der vom Betreiber zu treffenden Maßnahmen liegt - über mögliche Abhilfen einschließlich deren Kosten zu unterrichten.

(3) Betreiber eines öffentlichen Kommunikationsdienstes haben – unbeschadet der Bestimmungen des DSG 2000 – durch Datensicherheitsmaßnahmen jedenfalls Folgendes zu gewährleisten:

1. die Sicherstellung, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten;
2. den Schutz gespeicherter oder übermittelter personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe;
3. die Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten.

Die Regulierungsbehörde kann die von den Betreibern öffentlicher Kommunikationsdienste getroffenen Maßnahmen prüfen und Empfehlungen zum zu erreichenden Sicherheitsniveau abgeben.

Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 102/2011

§/Artikel/Anlage
§ 96

Inkrafttretensdatum
22.11.2011

Text

Datenschutz - Allgemeines

§ 96. (1) Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden.

(2) Die Übermittlung von im Abs. 1 genannten Daten darf nur erfolgen, soweit das für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber eines öffentlichen Kommunikationsdienstes erforderlich ist. Die Verwendung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie sonstige Übermittlungen dürfen nur auf Grund einer jederzeit widerrufbaren Zustimmung der Betroffenen erfolgen. Diese Verwendung ist auf das erforderliche Maß und den zur Vermarktung erforderlichen Zeitraum zu beschränken. Betreiber öffentlicher Kommunikationsdienste dürfen die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen.

(3) Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft im Sinne des § 3 Z 1 E-Commerce-Gesetz, BGBl. I Nr. 152/2001, sind verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er ermitteln, verarbeiten und übermitteln wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Ermittlung dieser Daten ist nur zulässig, wenn der Teilnehmer oder Nutzer seine Einwilligung dazu erteilt hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Der Teilnehmer ist auch über die Nutzungsmöglichkeiten auf Grund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren. Diese Information hat in geeigneter Form, insbesondere im Rahmen Allgemeiner Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen. Das Auskunftsrecht nach dem Datenschutzgesetz bleibt unberührt.

Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 27/2011

§/Artikel/Anlage
§ 97

Inkrafttretensdatum
19.05.2011

Text
Stammdaten

§ 97. (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.

(2) Stammdaten sind spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 102/2011

§/Artikel/Anlage
§ 98

Inkrafttretensdatum
22.11.2011

Text
Auskünfte an Betreiber von Notrufdiensten

§ 98. (1) Betreiber eines Kommunikationsnetzes oder –dienstes haben Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten im Sinne von § 92 Abs. 3 Z 3 lit. a bis d sowie über Standortdaten im Sinne des § 92 Abs. 3 Z 6 zu erteilen. In beiden Fällen ist Voraussetzung für die Zulässigkeit der

Übermittlung ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Die Notwendigkeit der Informationsübermittlung ist vom Betreiber des Notrufdienstes zu dokumentieren und dem Betreiber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nachzureichen. Der Betreiber darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Den Betreiber des Notrufdienstes trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens.

(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.

(3) Betreiber gemäß § 20 haben Betreibern von Notrufdiensten unmittelbar nach Eingang eines Notrufes Standortdaten im Sinne des § 92 Abs. 3 Z 6 der Telekommunikationsendeinrichtung, von der aus die Notrufnummer gewählt wurde, zugänglich zu machen und auf Anfrage Auskünfte über Stammdaten gemäß § 92 Abs. 3 Z 3 lit. a bis d zu erteilen.

(4) Betreiber von Kommunikationsnetzen haben bei der Ermittlung des Standortes der Telekommunikationsendeinrichtung entgeltfrei mitzuwirken, soweit hierfür internationale Standards vorhanden sind.

(5) Der Bundesminister für Verkehr, Innovation und Technologie kann mit Verordnung die näheren Details der Ermittlung, insbesondere die Genauigkeit und die Zuverlässigkeit der Standortermittlungen und Übertragung des Standortes der Telekommunikationsendeinrichtung festlegen. Hierbei hat er insbesondere auf internationale Standards, grundlegende Anforderungen im öffentlichen Interesse, die technischen Möglichkeiten und die hiefür erforderlichen Investitionen, allfällig bereits bestehende vertragliche Vereinbarungen zwischen Anbietern von Kommunikationsnetzen oder -diensten und Betreibern von Notrufdiensten sowie die Angemessenheit des erforderlichen wirtschaftlichen Aufwandes Bedacht zu nehmen.

Kurztitel

Telekommunikationsgesetz 2003

Kundmachungsorgan

BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 102/2011

§/Artikel/Anlage

§ 99

Inkrafttretensdatum

22.11.2011

Text

Verkehrsdaten

§ 99. (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.

(2) Sofern dies für Zwecke der Verrechnung von Endkunden- oder Vorleistungsentgelten erforderlich ist, hat der Betreiber eines öffentlichen Kommunikationsnetzes oder -dienstes Verkehrsdaten zu speichern. Die Verkehrsdaten sind zu löschen oder zu anonymisieren, sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten die Entgelte nicht schriftlich beeinsprucht wurden. Die Daten sind jedoch nicht zu löschen, wenn

1. ein fristgerechter Einspruch erhoben wurde, bis zum Ablauf jener Frist, innerhalb derer die Abrechnung rechtlich angefochten werden kann.

2. die Rechnung nicht beglichen wurde, bis zum Ablauf jener Frist, bis zu der der Anspruch auf Zahlung geltend gemacht werden kann, oder
3. ein Verfahren über die Höhe der Entgelte eingeleitet wurde, bis zur endgültigen Entscheidung.

Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle (§ 122) unverkürzt zur Verfügung zu stellen. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(3) Die Verarbeitung von Verkehrsdaten darf nur durch solche Personen erfolgen, die für die Entgeltverrechnung oder Verkehrsabwicklung, Behebung von Störungen, Kundenanfragen, Betrugsermittlung oder Vermarktung der Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen zuständig sind oder die von diesen Personen beauftragt wurden. Der Umfang der verwendeten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(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.

(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.

Kurztitel

Telekommunikationsgesetz 2003

Kundmachungsorgan

BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 27/2011

§/Artikel/Anlage

§ 102

Inkrafttretensdatum

19.05.2011

Text

Andere Standortdaten als Verkehrsdaten

§ 102. (1) Andere Standortdaten als Verkehrsdaten dürfen unbeschadet des § 98 nur verarbeitet werden, wenn sie

1. anonymisiert werden oder
2. die Benutzer oder Teilnehmer eine jederzeit widerrufbare Einwilligung gegeben haben.

(2) Selbst im Falle einer Einwilligung zur Verarbeitung von Daten gemäß Abs. 1 müssen die Benutzer oder Teilnehmer die Möglichkeit haben, diese Verarbeitung von Daten für jede Übertragung einfach und kostenlos zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß Abs. 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln. Unbeschadet des § 93 Abs. 3 ist die Ermittlung und Verwendung von Standortdaten, die nicht im Zusammenhang mit einem Kommunikationsvorgang stehen, zu Auskunftszwecken unzulässig.

Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 27/2011

§/Artikel/Anlage
§ 102a

Inkrafttretensdatum
01.04.2012

Text

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 Mobilfunkgerätekennung (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; *[Anm.: es fehlt die Zeit des eMail-Empfangs oder des Absendens, HGZ]*

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.

Kurztitel

Telekommunikationsgesetz 2003

Kundmachungsorgan

BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 27/2011

§/Artikel/Anlage

§ 102b

Inkrafttretensdatum

19.05.2011

Text

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.

Kurztitel
Telekommunikationsgesetz 2003

Kundmachungsorgan
BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 27/2011

§/Artikel/Anlage
§ 102c

Inkrafttretensdatum
19.05.2011

Text

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 DSG 2000 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 revisionssicher 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.

Kurztitel

Telekommunikationsgesetz 2003

Kundmachungsorgan

BGBl. I Nr. 70/2003 zuletzt geändert durch BGBl. I Nr. 102/2011

§/Artikel/Anlage

§ 107

Inkrafttretensdatum

22.11.2011

Text

Unerbetene Nachrichten

§ 107. (1) Anrufe - einschließlich das Senden von Fernkopien - zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers sind unzulässig. Der Einwilligung des Teilnehmers steht die Einwilligung einer Person, die vom Teilnehmer zur Benützung seines Anschlusses ermächtigt wurde, gleich. Die erteilte Einwilligung kann jederzeit widerrufen werden; der Widerruf der Einwilligung hat auf ein Vertragsverhältnis mit dem Adressaten der Einwilligung keinen Einfluss.

(1a) Bei Telefonanrufen zu Werbezwecken darf die Rufnummernanzeige durch den Anrufer nicht unterdrückt oder verfälscht werden und der Diensteanbieter nicht veranlasst werden, diese zu unterdrücken oder zu verfälschen.

(2) Die Zusendung einer elektronischen Post – einschließlich SMS – ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn

1. die Zusendung zu Zwecken der Direktwerbung erfolgt oder
2. an mehr als 50 Empfänger gerichtet ist.

(3) Eine vorherige Zustimmung für die Zusendung elektronischer Post gemäß Abs. 2 ist dann nicht notwendig, wenn

1. der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und
2. diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und
3. der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und
4. der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Eintragung in die in § 7 Abs. 2 E-Commerce-Gesetz genannte Liste, abgelehnt hat.

(4) *(Anm.: aufgehoben durch BGBl. I Nr. 133/2005)*

(5) Die Zusendung elektronischer Post zu Zwecken der Direktwerbung ist jedenfalls unzulässig, wenn

1. die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird, oder
2. die Bestimmungen des § 6 Abs. 1 E-Commerce-Gesetz verletzt werden, oder
3. der Empfänger aufgefordert wird, Websites zu besuchen, die gegen die genannte Bestimmung verstoßen oder
4. keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

(6) Wurden Verwaltungsübertretungen nach Absatz 1, 2 oder 5 nicht im Inland begangen, gelten sie als an jenem Ort begangen, an dem die unerbetene Nachricht den Anschluss des Teilnehmers erreicht.

Kurztitel

Telekommunikationsgesetz 2003

Kundmachungsorgan

BGBl. I Nr. 70/2003

§/Artikel/Anlage

§ 108

Inkrafttretensdatum

20.08.2003

Text

13. Abschnitt
Strafbestimmungen
Verletzung von Rechten der Benützer

§ 108. (1) Eine im § 93 Abs. 2 bezeichnete Person, die

1. unbefugt über die Tatsache oder den Inhalt des Telekommunikationsverkehrs bestimmter Personen einem Unberufenen Mitteilung macht oder ihm Gelegenheit gibt, Tatsachen, auf die sich die Pflicht zur Geheimhaltung erstreckt, selbst wahrzunehmen,
2. eine Nachricht fälscht, unrichtig wiedergibt, verändert, unterdrückt, unrichtig vermittelt oder unbefugt dem Empfangsberechtigten vorenthält,

ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.

(2) Der Täter ist nur auf Antrag des Verletzten zu verfolgen.

Kurztitel

Strafprozeßordnung 1975

Kundmachungsorgan

BGBl. Nr. 631/1975 zuletzt geändert durch BGBl. I Nr. 33/2011

§/Artikel/Anlage

§ 134

Inkrafttretensdatum

01.04.2012

Text

5. Abschnitt
Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten und von Personen
Definitionen

§ 134. Im Sinne dieses Bundesgesetzes ist

1. "Beschlagnahme von Briefen" das Öffnen und Zurückbehalten von Telegrammen, Briefen oder anderen Sendungen, die der Beschuldigte abschickt oder die an ihn gerichtet werden,
2. „Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs. 2 unterliegen, und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes),

2a. „Auskunft über Vorratsdaten" die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs. 2 bis 4 TKG zu speichern haben und die nicht nach § 99 Abs. 2 TKG einer Auskunft nach Z 2 unterliegen,

3. "Überwachung von Nachrichten" das Ermitteln des Inhalts von Nachrichten (§ 92 Abs. 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) ausgetauscht oder weitergeleitet werden,
4. "optische und akustische Überwachung von Personen" die Überwachung des Verhaltens von Personen unter Durchbrechung ihrer Privatsphäre und der Äußerungen von Personen, die nicht zur unmittelbaren Kenntnisnahme Dritter bestimmt sind, unter Verwendung technischer Mittel zur Bild- oder Tonübertragung und zur Bild- oder Tonaufnahme ohne Kenntnis der Betroffenen,
5. „Ergebnis" (der unter Z 1 bis 4 angeführten Beschlagnahme, Auskunft oder Überwachung) der Inhalt von Briefen (Z 1), die Daten einer Nachrichtenübermittlung, Vorratsdaten oder des Inhalts übertragener Nachrichten (Z 2 bis 3) und die Bild- oder Tonaufnahme einer Überwachung (Z 4).

Kurztitel
Strafprozeßordnung 1975

Kundmachungsorgan
BGBl. Nr. 631/1975 zuletzt geändert durch BGBl. I Nr. 33/2011

§/Artikel/Anlage
§ 135

Inkrafttretensdatum
01.04.2012

Text
Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten

§ 135. (1) Beschlagnahme von Briefen ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde.

(2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,
2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder
3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.
4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

(2a) Auskunft über Vorratsdaten (§§ 102a und 102b TKG) ist in den Fällen des Abs. 2 Z 2 bis 4 zulässig.

(3) Überwachung von Nachrichten ist zulässig,

1. in den Fällen des Abs. 2 Z 1,
2. in den Fällen des Abs. 2 Z 2, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Überwachung zustimmt,
3. wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen ansonsten wesentlich erschwert wäre und
   a. der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder einer Straftat gemäß §§ 278 bis 278b StGB dringend verdächtig ist, oder

b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat (lit. a) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;

4. in den Fällen des Abs. 2 Z 4.

Kurztitel

Strafprozeßordnung 1975

Kundmachungsorgan

BGBl.Nr. 631/1975 zuletzt geändert durch BGBl. I Nr. 19/2004

§/Artikel/Anlage

§ 136

Inkrafttretensdatum

01.01.2008

Text

Optische und akustische Überwachung von Personen

§ 136. (1) Die optische und akustische Überwachung von Personen ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Überwachung betroffene Person eine andere entführt oder sich ihrer sonst bemächtigt hat, und sich die Überwachung auf Vorgänge und Äußerungen zur Zeit und am Ort der Freiheitsentziehung beschränkt,
2. wenn sie sich auf Vorgänge und Äußerungen beschränkt, die zur Kenntnisnahme eines verdeckten Ermittlers oder sonst einer von der Überwachung informierten Person bestimmt sind oder von dieser unmittelbar wahrgenommen werden können, und sie zur Aufklärung eines Verbrechens (§ 17 Abs. 1 StGB) erforderlich scheint oder
3. wenn die Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder des Verbrechens der kriminellen Organisation oder der terroristischen Vereinigung (§§ 278a und 278b StGB) oder die Aufklärung oder Verhinderung von im Rahmen einer solchen Organisation oder Vereinigung begangenen oder geplanten strafbaren Handlungen oder die Ermittlung des Aufenthalts des wegen einer solchen Straftat Beschuldigten ansonsten aussichtslos oder wesentlich erschwert wäre und
   a. die Person, gegen die sich die Überwachung richtet, des mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder eines Verbrechens nach § 278a oder § 278b StGB dringend verdächtig ist oder
   b. auf Grund bestimmter Tatsachen anzunehmen ist, dass ein Kontakt einer solcherart dringend verdächtigen Person mit der Person hergestellt werde, gegen die sich die Überwachung richtet.

(2) Soweit dies zur Durchführung einer Überwachung nach Abs. 1 Z 3 unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte die betroffenen Räume benützen werde.

(3) Die optische Überwachung von Personen zur Aufklärung einer Straftat ist überdies zulässig,

1. wenn sie sich auf Vorgänge außerhalb einer Wohnung oder anderer durch das Hausrecht geschützter Räume beschränkt und ausschließlich zu dem Zweck erfolgt, Gegenstände oder Örtlichkeiten zu beobachten, um das Verhalten von Personen zu erfassen, die mit den Gegenständen in Kontakt treten oder die Örtlichkeiten betreten, oder
2. wenn sie ausschließlich zu dem in Z 1 erwähnten Zweck in einer Wohnung oder anderen durch das Hausrecht geschützten Räumen erfolgt, die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, ansonsten wesentlich erschwert wäre und der Inhaber dieser Wohnung oder Räume in die Überwachung ausdrücklich einwilligt.

(4) Eine Überwachung ist nur zulässig, soweit die Verhältnismäßigkeit (§ 5) gewahrt wird. Eine Überwachung nach Abs. 1 Z 3 zur Verhinderung von im Rahmen einer terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278a und 278b StGB) begangenen oder geplanten Straftaten ist überdies nur dann zulässig, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen.

Kurztitel
Strafprozeßordnung 1975

Kundmachungsorgan
BGBl. Nr. 631/1975 zuletzt geändert durch BGBl. I Nr. 33/2011

§/Artikel/Anlage
§ 137

Inkrafttretensdatum
01.04.2012

Text

Gemeinsame Bestimmungen

§ 137. (1) Eine Überwachung nach § 136 Abs. 1 Z 1 kann die Kriminalpolizei von sich aus durchführen. Die übrigen Ermittlungsmaßnahmen nach den §§ 135 und 136 sind von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen, wobei das Eindringen in Räume nach § 136 Abs. 2 jeweils im Einzelnen einer gerichtlichen Bewilligung bedarf.

(2) Bei der Beschlagnahme von Briefen sind die §§ 111 Abs. 4 und 112 sinngemäß anzuwenden.

(3) Ermittlungsmaßnahmen nach den §§ 135 und 136 dürfen nur für einen solchen künftigen, in den Fällen des § 135 Abs. 2 und 2a auch vergangenen, Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist. Eine neuerliche Anordnung ist jeweils zulässig, soweit auf Grund bestimmter Tatsachen anzunehmen ist, dass die weitere Durchführung der Ermittlungsmaßnahme Erfolg haben werde. Im Übrigen ist die Ermittlungsmaßnahme zu beenden, sobald ihre Voraussetzungen wegfallen.

Kurztitel
Strafprozeßordnung 1975

Kundmachungsorgan
BGBl. Nr. 631/1975 zuletzt geändert durch BGBl. I Nr. 33/2011

§/Artikel/Anlage
§ 138

Inkrafttretensdatum
01.04.2012

Text

§ 138. (1) Anordnung und gerichtliche Bewilligung einer Beschlagnahme von Briefen nach § 135 Abs. 1 haben die Bezeichnung des Verfahrens, den Namen des Beschuldigten, die Tat, deren der Beschuldigte verdächtig ist und ihre gesetzliche Bezeichnung sowie die Tatsachen, aus denen sich ergibt, dass die Anordnung oder Genehmigung zur Aufklärung der Tat erforderlich und verhältnismäßig ist, anzuführen; Anordnung und Bewilligung einer Ermittlungsmaßnahme nach den §§ 135 Abs. 2 bis 3 sowie 136 haben überdies zu enthalten:

1. die Namen oder sonstigen Identifizierungsmerkmale des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, oder der Person, deren Überwachung angeordnet wird,
2. die für die Durchführung der Ermittlungsmaßnahme in Aussicht genommenen Örtlichkeiten,
3. die Art der Nachrichtenübertragung, die technische Einrichtung und das Endgerät oder die Art der voraussichtlich für die optische und akustische Überwachung zu verwendenden technischen Mittel,
4. den Zeitpunkt des Beginns und der Beendigung der Überwachung,
5. die Räume, in die auf Grund einer Anordnung eingedrungen werden darf,
6. im Fall des § 136 Abs. 4 die Tatsachen, aus denen sich die schwere Gefahr für die öffentliche Sicherheit ergibt.

(2) Betreiber von Post- und Telegrafendiensten sind verpflichtet, an der Beschlagnahme von Briefen mitzuwirken und auf Anordnung der Staatsanwaltschaft solche Sendungen bis zum Eintreffen einer gerichtlichen Bewilligung zurückzuhalten; ergeht eine solche Bewilligung nicht binnen drei Tagen, so dürfen sie die Beförderung nicht weiter verschieben. Anbieter (§ 92 Abs. 1 Z 3 TKG) und sonstige Diensteanbieter (§§ 13, 16

und 18 Abs. 2 des E - Commerce - Gesetzes, BGBl. I Nr. 152/2001) sind verpflichtet, Auskunft über Daten einer Nachrichtenübermittlung (§ 135 Abs. 2) und über Vorratsdaten (§ 135 Abs. 2a) zu erteilen und an einer Überwachung von Nachrichten (§ 135 Abs. 3) mitzuwirken.

(3) Die Verpflichtung nach Abs. 2 und ihren Umfang sowie die allfällige Verpflichtung, mit der Anordnung und Bewilligung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten, hat die Staatsanwaltschaft dem Anbieter mit gesonderter Anordnung aufzutragen; diese Anordnung hat die entsprechende gerichtliche Bewilligung anzuführen. Die §§ 93 Abs. 2, 111 Abs. 3 sowie die Bestimmungen über die Durchsuchung gelten sinngemäß.

(4) Die Staatsanwaltschaft hat die Ergebnisse (§ 134 Z 5) zu prüfen und diejenigen Teile in Bild- oder Schriftform übertragen zu lassen und zu den Akten zu nehmen, die für das Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen (§§ 140 Abs. 1, 144, 157 Abs. 2).

(5) Nach Beendigung einer Ermittlungsmaßnahme nach den §§ 135 Abs. 2 bis 3 sowie 136 hat die Staatsanwaltschaft ihre Anordnung und deren gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung der Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen. Die Zustellung kann jedoch aufgeschoben werden, solange durch sie der Zweck dieses oder eines anderen Verfahrens gefährdet wäre. Wenn die Ermittlungsmaßnahme später begonnen oder früher beendet wurde als zu den in Abs. 1 Z 4 genannten Zeitpunkten, ist auch der Zeitraum der tatsächlichen Durchführung mitzuteilen.

Kurztitel
Strafprozeßordnung 1975

Kundmachungsorgan
BGBl.Nr. 631/1975 zuletzt geändert durch BGBl. I Nr. 109/2007

§/Artikel/Anlage
§ 139

Inkrafttretensdatum
01.01.2008

Text
§ 139. (1) Dem Beschuldigten ist zu ermöglichen, die gesamten Ergebnisse (§ 134 Z 5) einzusehen und anzuhören. Soweit berechtigte Interessen Dritter dies erfordern, hat die Staatsanwaltschaft jedoch Teile der Ergebnisse, die nicht für das Verfahren von Bedeutung sind, von der Kenntnisnahme durch den Beschuldigten auszunehmen. Dies gilt nicht, soweit während der Hauptverhandlung von den Ergebnissen Gebrauch gemacht wird.

(2) Die von der Durchführung der Ermittlungsmaßnahme betroffenen Personen haben das Recht, die Ergebnisse insoweit einzusehen, als ihre Daten einer Nachrichtenübermittlung, für sie bestimmte oder von ihnen ausgehende Nachrichten oder von ihnen geführte Gespräche oder Bilder, auf denen sie dargestellt sind, betroffen sind. Über dieses und das ihnen nach Abs. 4 zustehende Recht sind diese Personen, sofern ihre Identität bekannt oder ohne besonderen Verfahrensaufwand feststellbar ist, von der Staatsanwaltschaft zu informieren.

(3) Auf Antrag des Beschuldigten sind weitere Ergebnisse in Bild- oder Schriftform zu übertragen, wenn diese für das Verfahren von Bedeutung sind und ihre Verwendung als Beweismittel zulässig ist (§§ 140 Abs. 1, 144, 157 Abs. 2).

(4) Auf Antrag des Beschuldigten oder von Amts wegen sind Ergebnisse der Ermittlungsmaßnahme zu vernichten, wenn diese für ein Strafverfahren nicht von Bedeutung sein können oder als Beweismittel nicht verwendet werden dürfen. Dieses Antragsrecht steht auch den von der Ermittlungsmaßnahme Betroffenen zu, insoweit für sie bestimmte oder von ihnen ausgehende Nachrichten oder Bilder, auf denen sie dargestellt sind, oder von ihnen geführte Gespräche betroffen sind.

Kurztitel
Strafprozeßordnung 1975

Kundmachungsorgan
BGBl. Nr. 631/1975 zuletzt geändert durch BGBl. I Nr. 33/2011

§/Artikel/Anlage
§ 140

Inkrafttretensdatum
01.04.2012

Text

§ 140. (1) Als Beweismittel dürfen Ergebnisse (§ 134 Z 5), bei sonstiger Nichtigkeit nur verwendet werden,

1. wenn die Voraussetzungen für die Ermittlungsmaßnahme nach § 136 Abs. 1 Z 1 vorlagen,
2. wenn die Ermittlungsmaßnahme nach den §§ 135 oder 136 Abs. 1 Z 2 oder 3 oder Abs. 3 rechtmäßig angeordnet und bewilligt wurde (§ 137), und
3. in den Fällen des § 136 Abs. 1 Z 2 und 3 nur zum Nachweis eines Verbrechens (§ 17 Abs. 1 StGB),
4. in den Fällen der §§ 135 Abs. 1, Abs. 2 Z 2 bis 4, Abs. 2a, Abs. 3 Z 2 bis 4 nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, deretwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können.

(2) Ergeben sich bei Prüfung der Ergebnisse Hinweise auf die Begehung einer anderen strafbaren Handlung als derjenigen, die Anlass zur Überwachung gegeben hat, so ist mit diesem Teil der Ergebnisse ein gesonderter Akt anzulegen, soweit die Verwendung als Beweismittel zulässig ist (Abs. 1, § 144, § 157 Abs. 2).

(3) In anderen gerichtlichen und in verwaltungsbehördlichen Verfahren dürfen Ergebnisse nur insoweit als Beweismittel verwendet werden, als ihre Verwendung in einem Strafverfahren zulässig war oder wäre.

Kurztitel
Sicherheitspolizeigesetz

Kundmachungsorgan
BGBl. Nr. 566/1991 zuletzt geändert durch BGBl. I Nr. 13/2012

§/Artikel/Anlage
§ 16

Inkrafttretensdatum
01.04.2012

Text

3. Hauptstück
Begriffsbestimmungen
Allgemeine Gefahr; gefährlicher Angriff; Gefahrenerforschung

§ 16. (1) Eine allgemeine Gefahr besteht

1. bei einem gefährlichen Angriff (Abs. 2 und 3)
   oder
2. sobald sich drei oder mehr Menschen mit dem Vorsatz verbinden, fortgesetzt gerichtlich strafbare Handlungen zu begehen (kriminelle Verbindung).

(2) Ein gefährlicher Angriff ist die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich um einen Straftatbestand

1. nach dem Strafgesetzbuch (StGB), BGBl. Nr. 60/1974, ausgenommen die Tatbestände nach den §§ 278, 278a und 278b StGB, oder
2. nach dem Verbotsgesetz, StGBl. Nr. 13/1945, oder
3. nach dem Fremdenpolizeigesetz 2005 (FPG), BGBl. I Nr. 100, oder

4. nach dem Suchtmittelgesetz (SMG), BGBl. I Nr. 112/1997, ausgenommen der Erwerb oder Besitz von Suchtmitteln zum ausschließlichen persönlichen Gebrauch (§§ 27 Abs. 2, 30 Abs. 2 SMG), oder
5. nach dem Anti-Doping-Bundesgesetz 2007 (ADBG 2007), BGBl. I Nr. 30,

handelt.

(3) Ein gefährlicher Angriff ist auch ein Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung (Abs. 2) vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird.

(4) Gefahrenerforschung ist die Feststellung einer Gefahrenquelle und des für die Abwehr einer Gefahr sonst maßgeblichen Sachverhaltes.

Kurztitel

Sicherheitspolizeigesetz

Kundmachungsorgan

BGBl. Nr. 566/1991 zuletzt geändert durch BGBl. I Nr. 13/2012

§/Artikel/Anlage

§ 21

Inkrafttretensdatum

01.04.2012

Text

Gefahrenabwehr

§ 21. (1) Den Sicherheitsbehörden obliegt die Abwehr allgemeiner Gefahren.

(2) Die Sicherheitsbehörden haben gefährlichen Angriffen unverzüglich ein Ende zu setzen. Hiefür ist dieses Bundesgesetz auch dann maßgeblich, wenn bereits ein bestimmter Mensch der strafbaren Handlung verdächtig ist.

(3) Den Sicherheitsbehörden obliegt die erweiterte Gefahrenerforschung; das ist die Beobachtung

1. einer Person, die
   a) sich öffentlich oder in schriftlicher oder elektronischer Kommunikation für Gewalt gegen Menschen, Sachen oder die verfassungsmäßigen Einrichtungen ausspricht, oder
   b) sich Mittel und Kenntnisse verschafft, die sie in die Lage versetzen, Sachschäden in großem Ausmaß oder die Gefährdung von Menschen herbeizuführen,

   und damit zu rechnen ist, dass sie eine mit schwerer Gefahr für die öffentliche Sicherheit verbundene weltanschaulich oder religiös motivierte Gewalt herbeiführt, oder
2. einer Gruppierung, wenn im Hinblick auf deren bestehende Strukturen und auf zu gewärtigende Entwicklungen in deren Umfeld damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu weltanschaulich oder religiös motivierter Gewalt kommt.

Kurztitel
Sicherheitspolizeigesetz

Kundmachungsorgan
BGBl. Nr. 566/1991 zuletzt geändert durch BGBl. I Nr. 13/2012

§/Artikel/Anlage
§ 53

Inkrafttretensdatum
01.04.2012

Text

Zulässigkeit der Verarbeitung

§ 53. (1) Die Sicherheitsbehörden dürfen personenbezogene Daten ermitteln und weiterverarbeiten

1. für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§ 19);
2. für die Abwehr krimineller Verbindungen (§§ 16 Abs. 1 Z 2 und 21);

2a. für die **erweiterte** Gefahrenerforschung (§ 21 Abs. 3) unter den Voraussetzungen des § 91c Abs. 3;

3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenerforschung (§ 16 Abs. 4 und § 28a);
4. für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§ 22 Abs. 2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;
5. für Zwecke der Fahndung (§ 24);
6. um bei einem bestimmten Ereignis die öffentliche Ordnung aufrechterhalten zu können;
7. für die **Analyse und Bewertung der Wahrscheinlichkeit einer Gefährdung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit** durch die Verwirklichung eines Tatbestandes nach dem Vierzehnten und Fünfzehnten Abschnitt des Strafgesetzbuches.

(2) Die Sicherheitsbehörden dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen verarbeitet haben, für die Zwecke und unter den Voraussetzungen nach Abs. 1 ermitteln und weiterverarbeiten; ein automationsunterstützter Datenabgleich im Sinne des § 141 StPO ist ihnen jedoch untersagt. Bestehende Übermittlungsverbote bleiben unberührt.

(3) Die Sicherheitsbehörden sind berechtigt, von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechtes und den von diesen betriebenen Anstalten Auskünfte zu verlangen, die sie für die Abwehr gefährlicher Angriffe, für die erweiterte Gefahrenerforschung unter den Voraussetzungen nach Abs. 1 oder für die Abwehr krimineller Verbindungen benötigen. Eine Verweigerung der Auskunft ist nur zulässig, soweit andere öffentliche Interessen die Abwehrinteressen überwiegen oder eine über die Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) hinausgehende sonstige gesetzliche Verpflichtung zur Verschwiegenheit besteht.

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

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

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

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

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

(3c) **In den Fällen der Abs. 3a und 3b trifft die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens.** Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und im Fall des Abs. 3b gegen Ersatz der Kosten nach der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004, zu erteilen. Im Falle des Abs. 3b hat die Sicherheitsbehörde dem Betreiber überdies unverzüglich, spätestens innerhalb von 24 Stunden eine schriftliche Dokumentation nachzureichen. **In den Fällen des Abs. 3a Z 3 sowie Abs. 3b ist die Sicherheitsbehörde verpflichtet, den Betroffenen darüber zu informieren, dass eine Auskunft zur Zuordnung seines Namens oder seiner Anschrift zu einer bestimmten IP-Adresse (§ 53 Abs. 3a Z 3) oder zur Standortbeauskunftung (§ 53 Abs. 3b) eingeholt wurde, sofern hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 erforderlich war.** Dabei sind dem Betroffenen nachweislich und ehestmöglich die Rechtsgrundlage sowie das Datum und die Uhrzeit der Anfrage bekannt zu geben. Die Information Betroffener kann aufgeschoben werden, solange durch sie der Ermittlungszweck gefährdet wäre, und kann unterbleiben, wenn der Betroffene bereits nachweislich Kenntnis erlangt hat oder die Information des Betroffenen unmöglich ist.

(3d) Die Sicherheitsbehörden sind zur Vorbeugung und Abwehr gefährlicher Angriffe gegen die Umwelt berechtigt, von Behörden des Bundes, der Länder und Gemeinden Auskünfte über von diesen genehmigte Anlagen und Einrichtungen zu verlangen, bei denen wegen der Verwendung von Maschinen oder Geräten, der Lagerung, Verwendung oder Produktion von Stoffen, der Betriebsweise, der Ausstattung oder aus anderen Gründen besonders zu befürchten ist, dass im Falle einer Abweichung der Anlage oder Einrichtung von dem der Rechtsordnung entsprechenden Zustand eine Gefahr für das Leben, die Gesundheit mehrerer Menschen oder in großem Ausmaß eine Gefahr für Eigentum oder Umwelt entsteht. Die ersuchte Behörde ist verpflichtet, die Auskunft zu erteilen.

(4) Abgesehen von den Fällen der Abs. 2 bis 3b und 3d sind die Sicherheitsbehörden für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff auf allgemein zugängliche Daten, zu ermitteln und weiterzuverarbeiten.

(5) Die Sicherheitsbehörden sind im Einzelfall und unter den Voraussetzungen des § 54 Abs. 3 ermächtigt, für die Abwehr gefährlicher Angriffe und krimineller Verbindungen, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen, für die erweiterte Gefahrenerforschung (§ 21 Abs. 3) und zur Fahndung (§ 24) personenbezogene Bilddaten zu verwenden, die Rechtsträger des öffentlichen oder privaten Bereichs mittels Einsatz von Bild- und Tonaufzeichnungsgeräten rechtmäßig ermittelt und den Sicherheitsbehörden übermittelt haben. Dabei ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren. Nicht zulässig ist die Verwendung von Daten über nichtöffentliches Verhalten.

Kurztitel
Urheberrechtsgesetz

Kundmachungsorgan
BGBl.Nr. 111/1936 zuletzt geändert durch BGBl. I Nr. 81/2006

§/Artikel/Anlage
§ 87b

Inkrafttretensdatum
22.06.2006

Text

Anspruch auf Auskunft

§ 87b. (1) Wer im Inland Werkstücke verbreitet, an denen das Verbreitungsrecht durch In-Verkehr-Bringen in einem Mitgliedstaat der Europäischen Gemeinschaft oder in einem Vertragsstaat des Europäischen Wirtschaftsraums erloschen ist (§ 16 Abs. 3), hat dem Berechtigten auf Verlangen richtig und vollständig Auskunft über Hersteller, Inhalt, Herkunftsland und Menge der verbreiteten Werkstücke zu geben. Anspruch auf Auskunft hat, wem das Recht, die Werkstücke im Inland zu verbreiten, im Zeitpunkt des Erlöschens zugestanden ist.

(2) Wer in einem auf dieses Gesetz gegründeten Ausschließungsrecht verletzt worden ist, kann Auskunft über den Ursprung und die Vertriebswege der rechtsverletzenden Waren und Dienstleistungen verlangen, sofern dies nicht unverhältnismäßig im Vergleich zur Schwere der Verletzung wäre und nicht gegen gesetzliche Verschwiegenheitspflichten verstoßen würde; zur Erteilung der Auskunft sind der Verletzer und die Personen verpflichtet, die gewerbsmäßig

1. rechtsverletzende Waren in ihrem Besitz gehabt,
2. rechtsverletzende Dienstleistungen in Anspruch genommen oder
3. für Rechtsverletzungen genutzte Dienstleistungen erbracht haben.

(2a) Die Pflicht zur Auskunftserteilung nach Abs. 2 umfasst, soweit angebracht,

1. die Namen und Anschriften der Hersteller, Vertreiber, Lieferanten und der anderen Vorbesitzer der Waren oder Dienstleistungen sowie der gewerblichen Abnehmer und Verkaufsstellen, für die sie bestimmt waren,
2. die Mengen der hergestellten, ausgelieferten, erhaltenen oder bestellten Waren und die Preise, die für die Waren oder Dienstleistungen bezahlt wurden.

(3) Vermittler im Sinn des § 81 Abs. 1a haben dem Verletzten auf dessen schriftliches und ausreichend begründetes Verlangen Auskunft über die Identität des Verletzers (Name und Anschrift) beziehungsweise die zur Feststellung des Verletzers erforderlichen Auskünfte zu geben. In die Begründung sind insbesondere hinreichend konkretisierte Angaben über die den Verdacht der Rechtsverletzung begründenden Tatsachen aufzunehmen. Der Verletzte hat dem Vermittler die angemessenen Kosten der Auskunftserteilung zu ersetzen.

(4) Vertreter des Kunstmarkts, die an einer dem Folgerecht unterliegenden Veräußerung im Sinn des § 16b Abs. 2 beteiligt waren, haben dem Berechtigten auf Verlangen richtig und vollständig alle Auskünfte zu geben, die für die Sicherung der Zahlung aus dieser Veräußerung erforderlich sein können. Der Anspruch erlischt, wenn die Auskünfte nicht in einem Zeitraum von drei Jahren nach der Weiterveräußerung verlangt werden.

Kurztitel
E-Commerce-Gesetz

Kundmachungsorgan
BGBl. I Nr. 152/2001

§/Artikel/Anlage
§ 16

Inkrafttretensdatum
01.01.2002

Text

Ausschluss der Verantwortlichkeit bei Speicherung fremder Inhalte (Hosting)

§ 16. (1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert, ist für die im Auftrag eines Nutzers gespeicherten Informationen nicht verantwortlich, sofern er

1. von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er diese Kenntnis oder dieses Bewusstsein erhalten hat, unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

(2) Abs. 1 ist nicht anzuwenden, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Kurztitel
E-Commerce-Gesetz

Kundmachungsorgan
BGBl. I Nr. 152/2001

§/Artikel/Anlage
§ 18

Inkrafttretensdatum
01.01.2002

Text

Umfang der Pflichten der Diensteanbieter

§ 18. (1) Die in den §§ 13 bis 17 genannten Diensteanbieter sind nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

(2) Die in den §§ 13 und 16 genannten Diensteanbieter haben auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem alle Informationen zu übermitteln, an Hand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können.

(3) Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet.

(4) Die in § 16 genannten Diensteanbieter haben den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

(5) Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt.