Bundesministerium
der Justiz und
für Verbraucherschutz

Leitlinien

des BMJV zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten

15. April 2015

Grundkonzept:

Im Telekommunikationsgesetz (TKG) wird eine eng begrenzte Pflicht für alle TK-Anbieter zur Speicherung von genau bezeichneten Verkehrsdaten mit Ausnahme von Diensten der elektronischen Post eingeführt. Diese gespeicherten Daten müssen unverzüglich nach Ablauf der Speicherfrist gelöscht werden.

In der Strafprozessordnung (StPO) wird der Abruf dieser Daten mit einem engen Straftatenkatalog, strengen Richtervorbehalt und weiteren, eng definierten Voraussetzungen zur Gewährleistung der Grundrechte und der Verhältnismäßigkeit geregelt.

Oberste Richtschnur aller Regelungen sind die strengen Vorgaben des Bundesverfassungsgerichtes und des Europäischen Gerichtshofes.

Welche Daten müssen gespeichert werden?

Gespeichert werden müssen im TKG genau bezeichnete Verkehrsdaten, die bei der Telekommunikation anfallen. Das sind insbesondere die Rufnummern der beteiligten Anschlüsse, Zeitpunkt und Dauer des Anrufs, bei Mobilfunk auch die Standortdaten, sowie IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP-Adresse (vgl. im Einzelnen Anlage 1 „Datenkranz“).

Nicht gespeichert werden dürfen:

- Inhalt der Kommunikation,
- aufgerufene Internetseiten und
- Daten von Diensten der elektronischen Post

Wie lange müssen die Daten gespeichert werden?

Hinsichtlich der Speicherdauer wird differenziert zwischen den Standortdaten und den weiteren Verkehrsdaten. Für die Standortdaten wird eine Speicherfrist von vier Wochen, im Übrigen eine Speicherfrist von zehn Wochen bestimmt.

Warum müssen Standortdaten nur für kurze Zeit gespeichert werden?

Standortdaten sind besonders sensible Daten, weil sie Auskunft darüber geben, in welcher Funkzelle sich ein Mobiltelefon bei einem Kommunikationsvorgang befindet. Über die Funkzelle kann der Aufenthaltsort des Mobilfunkteilnehmers auf einen Umkreis von zum Teil unter einem Kilometer bestimmt werden. Die Kenntnis von Standortdaten ermöglicht die Erstellung von Bewegungs- bis hin zu Persönlichkeitsprofilen.
Deshalb schaffen wir sowohl für die zu speichernden Standortdaten als auch für die aus geschäftlichen Gründen vorhandenen Standortdaten gegenüber den sonstigen Verkehrsdaten einschränkende Regelungen:

Bewegungs- und Persönlichkeitsprofile dürfen nicht erstellt werden. Um die Erstellung von Profilen auf der Grundlage der zu speichernden Daten schon von vornherein auszuschließen, wird für Standortdaten nur eine kurze Speicherfrist vorgesehen. Außerdem dürfen nur einzelne Standortdaten abgerufen werden. Ferner wird gewährleistet, dass bei der gerichtlichen Prüfung der Verhältnismäßigkeit ein strenger Maßstab angelegt wird. Im Anordnungsbeschluss sind einzelfallbezogen die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme darzulegen.

Für den Abruf von aus geschäftlichen Gründen vorhandenen Standortdaten sollen auch im Übrigen die gleichen strengen gesetzlichen Voraussetzungen wie für den Abruf der verpflichtend gespeicherten Daten gelten. Das heißt insbesondere, dass ein Abruf nur bei schwersten Straftaten zulässig ist und unter einem strengen Richtervorbehalt steht. Zudem dürfen nur Daten aus den letzten vier Wochen vor der Abfrage abgerufen werden, auch wenn noch ältere Daten vorhanden sind. Damit erhöhen wir gegenüber der geltenden Rechtslage den Schutz von persönlichen Daten der Bürgerinnen und Bürger.

Wer ist berechtigt, die gespeicherten Daten abzurufen?

Die Strafverfolgungsbehörden dürfen die gespeicherten Daten zu engdefinierten Strafverfolgungszwecken abrufen. Den Ländern wird ermöglicht, einen Abruf der Verkehrsdaten in ihren Polizeigesetzen zu regeln, wenn tatsächliche Anhaltspunkte für bestimmte konkrete schwerste Gefahren vorliegen.

Wie werden die Grundrechte der Betroffenen auf Datenschutz, Achtung des Privatlebens und des Telekommunikationsgeheimnisses sowie auf informationelle Selbstbestimmung geschützt?

Zum Schutz der Grundrechte der Bürgerinnen und Bürger, deren Daten gespeichert werden, sehen die Leitlinien folgende Bestimmungen vor:

- Schutz von Berufsgeheimnisträgern beim Abruf der Daten durch Verwendungs- und Verwertungsverbote,
- Datenabruf nur bei schwersten Straftaten,
- strenger Richtervorbehalt mit Verhältnismäßigkeitsprüfung und ohne Eilkompetenz der Staatsanwaltschaft,
- Transparenz und Rechtsschutzmöglichkeiten für diejenigen, deren Daten abgerufen werden,
- besonders hohe Anforderungen an Datenschutz und Datensicherheit bei den speicherverpflichteten TK-Anbietern,
- Löschverpflichtung nach Ablauf der Höchstspeicherfrist.

Vgl. dazu jeweils im Einzelnen die folgenden Ausführungen.

Wie werden Berufsgeheimnisträger geschützt?

Verkehrsdaten, die sich auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen beziehen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, sind grundsätzlich von der Speicherpflicht ausgenommen. Darüber hinaus dürfen Verkehrsdaten in Bezug auf alle nach § 53 StPO zeugnisverweigerungsberechtigten Personen (Seelsorger, Rechtsanwälte, Ärzte, Apotheker, Beratungsstellen für Betäubungsmittelabhängigkeit und Schwangerschaftskonflikte, Abgeordnete, Presse) nicht abgerufen werden. Zufallsfunde unterliegen einem Verwertungsverbot.

Warum kann im TKG keine Möglichkeit vorgesehen werden, alle Berufsgeheimnisträger von der Speicherpflicht auszunehmen?

Wie auch im Deutschen Bundestag schon zutreffend vorgetragen wurde, ist es unter Datenschutzgesichtspunkten nicht vertretbar, eine Art Datenbank mit Berufsgeheimnisträgern und ihren Rufnummern anzulegen und bei allen TK-Anbietern zu hinterlegen. Der Eingriff in deren Berufsfreiheit und ihr Recht auf informationelle Selbstbestimmung wäre größer als der Nutzen, der in der Ausnahme von der Speicherung liegt. Bei dynamischen IP-Adressen ist eine Ausnahme technisch gar nicht möglich.

In Bezug auf welche Straftaten ist der Abruf der Daten zulässig?

Der Abruf der Daten ist nur zur Verfolgung von katalogmäßig aufgeführten schwersten Straftaten zulässig, die auch im Einzelfall schwer wiegen müssen. Dabei ist der Katalog im Vergleich zu dem Katalog, der nach der vorhergehenden, vom BVerfG verworfenen Regelung maßgeblich war, deutlich reduziert und lehnt sich an den Katalog zur Wohnraumüberwachung an. Erfasst werden insbesondere terroristische Straftaten und Straftaten gegen höchstpersönliche Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexuelle Selbstbestimmung (siehe im Einzelnen Anlage 2 „Straftatenkatalog“).

Ist ein Richtervorbehalt vorgesehen?

Die Leitlinien sehen einen umfassenden Richtervorbehalt für den Abruf der Daten durch die Strafverfolgungsbehörden vor. Eine Eilkompetenz der Staatsanwaltschaft besteht – wie bei der Wohnraumüberwachung nach §§ 100c, 100d StPO – nicht.

Erfahren die Betroffenen von dem Abruf der Daten?

Der Abruf der Daten ist keine verdeckte Maßnahme. Die betroffenen Personen sind grundsätzlich vor dem Abruf der Daten zu benachrichtigen. Ist eine heimliche Verwendung nach gerichtlicher Prüfung ausnahmsweise zulässig, bedarf es einer nachträglichen Benachrichtigung, von der nur mit richterlicher Bestätigung abgesehen werden kann.

Ist die Sicherheit der gespeicherten Daten gewährleistet?

Die nach dem Stand der Technik höchstmögliche Sicherheit der Daten ist zu gewährleisten. Die Speicherung hat im Inland zu erfolgen. Die Anbieter müssen die Daten gegen unbefugte Kenntnisnahme und Verwendung schützen. Konkret erforderlich sind insbesondere der Einsatz eines besonders sicheren Verschlüsselungsverfahrens, die Speicherung in gesonderten Speichereinrichtungen mit einem hohen Schutz vor Zugriffen aus dem Internet, die revisionssichere Protokollierung des Zugriffs sowie die Gewährleistung des Vier-Augen-Prinzips für den Zugriff auf die Daten. Daneben sind detaillierte Löschungsvorschriften sowohl für die TK-Anbieter als auch für die Strafverfolgungsbehörden vorzusehen.

Was geschieht mit den Daten nach Ablauf der Höchstspeicherfrist?

Die besonders gesicherten Daten sind nach Ablauf der Speicherfrist zu löschen. Kommt der TK-Anbieter der Löschverpflichtung nicht nach, wird dies mit einem Ordnungsgeld belegt.

Welche weiteren Sanktionen gibt es gegen Rechtsverstöße?

Wer sich nicht an die Bestimmungen zur Sicherung und zum Schutz der Daten hält, wird mit Sanktionen belegt.

Den Handel mit gestohlenen Daten werden wir unter Strafe stellen. Wir schaffen dazu einen neuen Straftatbestand der „Datenhehlerei“. Damit schließen wir eine Strafbarkeitslücke.

Werden die TK-Anbieter entschädigt?

Wenn erkennbar oder substantiiert vorgebracht ist, dass für die TK-Anbieter durch die Speicherung eine unverhältnismäßige Kostenlast entsteht, die in solcher Weise erdrosselnde Wirkung hat, dass das Übermaßverbot verletzt ist, werden sie für die Umsetzung der Speicherverpflichtung entschädigt. Für Kosten, die durch den Abruf der Daten entstehen, wird eine Entschädigungsregelung vorgesehen.

Ist die vorgeschlagene Einführung einer Höchstspeicherfrist für Verkehrsdaten mit den Vorgaben des Bundesverfassungsgerichts und des Europäischen Gerichtshofs vereinbar?

Die Vorgaben des Bundesverfassungsgerichts und des Europäischen Gerichtshofs halten wir ein. Die vorgeschlagene Regelung ist deutlich enger als die alte EU-Richtlinie zur Vorratsdatenspeicherung. Es werden weniger Daten für einen deutlich kürzeren Zeitraum gespeichert. Es sollen bei weitem nicht alle Daten gespeichert werden. Die Daten von Diensten der elektronischen Post sind komplett ausgenommen. Hinsichtlich der Speicherfrist wird – ausgehend von der Sensibilität der Daten für den Bürger – nach Datenarten differenziert: Die Höchstspeicherfrist für Standortdaten beträgt vier Wochen, für die übrigen Verkehrsdaten zehn Wochen. Auch für den Zugriff auf die Daten errichten wir mit striktem Richtervorbehalt, sehr engem Straftatenkatalog und Substantiierungsanforderungen hohe Hürden. Auf Standortdaten darf nur einzeln zugegriffen wer-

den; Bewegungsprofile sind nicht möglich. Grundrechtseingriffe werden auf das absolut Notwendige beschränkt. Darüber hinaus gewährleisten wir für die Bürgerinnen und Bürger Datensicherheit, Transparenz und effektiven Rechtsschutz. Berufsgeheimnisträger werden besonders geschützt.

Datenkranz Anlage 1

- Telefondienste

1. die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2. Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone von Beginn und Ende der Verbindung,
3. Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,
4. im Fall mobiler Telefondienste ferner

   a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,

   b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,

   c) die Bezeichnung der Funkzellen, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt werden,

   d) Datum und Uhrzeit der ersten Aktivierung des Dienstes sowie die Bezeichnung der Funkzelle, wenn Dienste im Voraus bezahlt wurden,
5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.

Bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht.

- Anbieter von öffentlich zugänglichen Internetzugangsdiensten

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung.

Straftatenkatalog Anlage 2

Die nach § [...] TKG gespeicherten Verkehrsdaten dürfen erhoben werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Satz 2 bezeichnete, schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, und die Tat auch im Einzelfall schwer wiegt, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Schwere Straftaten im Sinne des Satzes 1 sind:

1. aus dem Strafgesetzbuch:

a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80, 81, 82, 89a, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,

b) besonders schwerer Fall des Landfriedensbruchs nach § 125a, Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 4 Halbsatz 2 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 Alternative 1, jeweils auch in Verbindung mit § 129b Absatz 1,

c) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b, 177 Absatz 2 Nummer 2 und des § 179 Absatz 5 Nummer 2,

d) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften in den Fällen des § 184b Absatz 3, § 184c Absatz 3,

e) Mord und Totschlag nach den §§ 211 und 212,

f) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, §§ 239a, 239b und Menschenhandel zum Zweck der sexuellen Ausbeutung und zum Zweck der Ausbeutung der Arbeitskraft nach § 232 Absatz 3, Absatz 4 oder Absatz 5, § 233 Absatz 3, jeweils soweit es sich um Verbrechen handelt,

g) schwerer Bandendiebstahl nach § 244a Absatz 1, schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251, räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen, gewerbsmäßige Bandenhehlerei

nach § 260a Absatz 1, besonders schwerer Fall der Geldwäsche nach § 261 unter den in § 261 Absatz 4 Satz 2 genannten Voraussetzungen,

h) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Absatz 1 bis 3, des § 308 Absatz 1 bis 3, des § 309 Absatz 1 bis 4, des § 310 Absatz 1, der §§ 313, 314, 315 Absatz 3, des § 315b Absatz 3 sowie der §§ 316a und 316c,

2. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Absatz 2,

b) Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,

3. aus dem Betäubungsmittelgesetz:

a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,

b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2 und 4, § 30a,

4. aus dem Grundstoffüberwachungsgesetz:
eine Straftat nach § 19 Absatz 1 unter den in § 19 Absatz 3 Satz 2 genannten Voraussetzungen,

5. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,

b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,

6. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

7. aus dem Waffengesetz:

a) besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,

b) besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5.