Datenproduzent Handy

The mobile phone – producer of data

Mobiles Tagesprotokoll

Laut einer Studie von Marketagent aus dem Jahr 2010 verschicken österreichische HandybesitzerInnen zwischen 14 und 27 Jahren täglich rund 15 SMS und telefonieren 37,5 Minuten. Dabei fallen auch jede Menge Verkehrs- und Standortdaten an.
Wie schaut es bei dir aus? Trägst du so wie 80% aller österreichischen HandybesitzerInnen dein Handy immer bei dir? Und vor allem – welche Verkehrs- und Standortdaten produzierst du an einem normalen Tag?

Trag für die Dauer eines Tages jeden Anruf und jede Nachricht in die nachfolgende Tabelle ein.
Zur Erklärung: „Ein" steht für „eingehende Anrufe bzw. Nachrichten", die du erhältst,
„Aus" steht für „ausgehende Anrufe und Nachrichten", die du tätigst.

Anruf				SMS MMS		
Ein	**Aus**	**Uhrzeit**	**Dauer in min.**	**Uhr-zeit**	**Mein Kommunikationspartner**	**Mein Standort**

Mobile daily record

In Austria owners of mobile phones between the age of 14 and 27 send approx. 15 text messages and make phone calls for 37.5 minutes per day. This way quite a lot of traffic data and location data is created.
What about you? Do you always carry your mobile phone with you, like 80% of all owners of mobile phones in Austria? Even more so, what traffic data and location data do you create on an average day?

Enter every call you make and every message you send in one day into the table below.
Explanation: „In" means „incoming calls and/or messages" you receive, „out" means „outgoing calls and messages" you make/send.

		Call		Text/Multi-media message		
In	**Out**	**Time**	**Dura-tion in min.**	**Time**	**My communication partner**	**My location**

Richtig kombiniert?

Verbinde die richtigen Satzteile!

Wenn jemand weiß, mit wem du telefonierst,	kann man aus den Standortdaten deines Handys ablesen.
Wer über die zeitliche Nutzung deines Handys Bescheid weiß,	kann er daraus auf deinen Freundes- und Bekanntenkreis schließen.
Wie oft und wie lang du mit jemandem telefonierst,	verraten nichts über Gesprächs- oder Nachrichteninhalte.
Wo du den lieben langen Tag unterwegs bist,	ist auch über deinen Tagesablauf informiert.
Die Verkehrs- und Standortdaten deines Telefons	zeigt, wie wichtig dir diese Person ist.

FORUM MOBILKOMMUNIKATION

The right connection?

Connect the correct phrases!

If somebody knows whom you call	can be seen from the location data of your mobile phone.
A person who knows the time when you use your mobile phone	he can get an idea of your contacts and friends.
The frequency and duration of your phone calls	do not tell anything about the contents of your calls or messages.
Your whereabouts during the day	also knows about your daily routine.
The traffic data and location data of your mobile phone	shows how important that person is to you.

Arbeitsblatt 10

Smart & Safe

FMK FORUM MOBILKOMMUNIKATION

Freier Zugriff? – Die Gesetzeslage

Welche Daten von einem Telekommunikationsanbieter gespeichert werden und was mit ihnen geschehen darf, ist im Telekommunikationsgesetz geregelt. Nachfolgend findest du einige Auszüge aus dem Gesetz.

Stammdaten

§ 97. (1) Stammdaten dürfen 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 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.

Auskünfte an Betreiber von Notrufdiensten

§ 98. (1) Betreiber eines Kommunikationsnetzes oder -dienstes haben Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten sowie über Standortdaten 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 betroffenen 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.

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. [...]

(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. [...]

(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.

Inhaltsdaten

§ 101. (1) Inhaltsdaten dürfen - sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt - grundsätzlich nicht gespeichert werden. Sofern aus technischen Gründen eine kurzfristige Speicherung erforderlich ist, hat der Anbieter nach Wegfall dieser Gründe die gespeicherten Daten unverzüglich zu löschen.

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.

Auszüge aus dem Telekommunikationsgesetz (Fassung 15.5.213), zitiert nach
www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20002849/TKG%202003%2c%20Fassung%20vom%2005.04.2012.pdf

Wer hat Zugriff?

Entscheide, ob die Aussagen richtig oder falsch sind. Ergänze in der rechten Spalte die richtige Aussage, falls du dich für „falsch“ entscheidest.

	richtig	falsch	richtige Aussage
Geht ein Notruf bei einem Notrufdienst ein, müssen unmittelbar danach die Standortdaten vom Telefon, das den Notruf abgesetzt hat, bekanntgegeben werden.			
Inhaltsdaten dürfen für Verrechnungszwecke gespeichert werden.			
Inhaltsdaten dürfen nur gespeichert werden, wenn sie wesentlicher Bestandteil eines Kommunikationsdienstes sind.			
Kann ein Unglück nur verhindert werden, weil die Standortdaten einer bestimmten Person bzw. ihres Telefons bekannt sind, so dürfen diese Daten an Notrufdienste weitergegeben werden.			
Stammdaten dürfen an andere Unternehmen für Werbezwecke verkauft werden.			
Stammdaten dürfen auch nach Auflösung eines Vertrages verwendet werden, um Werbung zu versenden.			
Stammdaten dürfen bei Notfällen an Notrufdienste weitergegeben werden.			
Stammdaten dürfen für die Erstellung einer Rechnung verwendet werden.			
Telekommunikationsanbieter dürfen Stamm- und Standortdaten nur an Notrufdienste weitergeben, nachdem sie eine schriftliche Dokumentation der Notwendigkeit dieser Weitergabe erhalten haben.			
Verkehrsdaten dürfen für Verrechnungszwecke gespeichert werden.			
Verkehrsdaten müssen ausnahmslos nach drei Monaten gelöscht werden.			
Kann ein Unglück nur verhindert werden, weil man die Inhaltsdaten einer bestimmten Person bzw. eines Telefons kennt, so dürfen diese Daten an Notrufdienste weitergegeben werden.			

FORUM MOBILKOMMUNIKATION

Free access?
The legal situation

The Austrian Telecommunications Act [Telekommunikationsgesetz] regulates which data a telecommunications provider may store and how such data may be used.

Stammdaten

§ 97. (1) Stammdaten dürfen 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 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.

Auskünfte an Betreiber von Notrufdiensten

§ 98. (1) Betreiber eines Kommunikationsnetzes oder -dienstes haben Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten sowie über Standortdaten 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 betroffenen 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.

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. [...]

(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. [...]

(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.

Inhaltsdaten

§ 101. (1) Inhaltsdaten dürfen - sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt - grundsätzlich nicht gespeichert werden. Sofern aus technischen Gründen eine kurzfristige Speicherung erforderlich ist, hat der Anbieter nach Wegfall dieser Gründe die gespeicherten Daten unverzüglich zu löschen.

Auszüge aus dem Telekommunikationsgesetz (Fassung 15.5.2013), zitiert nach
www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20002849/TKG%202003%2c%20Fassung%20vom%2005.04.2012.pdf

Free access?

Decide whether the statements are true or false. Add the correct statement if you decide that the statement is „false".

	true	false	correct statement
If an emergency service receives an emergency call, the location data of the phone from which the call was made must be advised immediately thereafter.			
Content data may be stored for accounting purposes.			
Content data may be stored only if they are a material component of a communication service.			
If an accident can be prevented only because the location data of a certain person and/or of his/her phone are known, such data may be passed on to emergency services.			
Master data may be sold to other enterprises for advertising purposes.			
Master data may be used also after termination of a contract in order to send advertisements.			
In emergency cases master data may be passed on to emergency services.			
Master data may be used to prepare a bill.			
Telecommunications providers may pass on master data and location data only to emergency services after they have received a written documentation of the necessity of such a transfer.			
Traffic data may be stored for accounting purposes.			
Traffic data must be deleted after three months, even if bills are still outstanding.			
If an accident can be prevented only because the content data of a certain person and/or of a phone are known, such data may be passed on to emergency services.			

Words to help you:

accounting purposes – *Rechnungszweck*

Wer hat Zugriff?

	richtig	falsch	richtige Aussage
Geht ein Notruf bei einem Notrufdienst ein, müssen unmittelbar danach automatisch die Standortdaten vom Telefon, das den Notruf abgesetzt hat, bekanntgegeben werden.		X	Die Standortdaten müssen weitergegeben werden, wenn diese zur Hilfeleistung notwendig sind und die AnruferIn diese nicht mitteilen kann.
Inhaltsdaten dürfen für Verrechnungszwecke gespeichert werden.		X	Inhaltsdaten dürfen grundsätzlich nicht gespeichert werden. Ausnahme ist, wenn aus technischen Gründen eine kurzfristige Speicherung notwendig ist.
Inhaltsdaten dürfen nur gespeichert werden, wenn sie wesentlicher Bestandteil eines Kommunikationsdienstes sind.	X		
Kann ein Unglück nur verhindert werden, weil die Standortdaten einer bestimmten Person bzw. ihres Telefons bekannt sind, so dürfen diese Daten an Notrufdienste weitergegeben werden.	X		
Stammdaten dürfen an andere Unternehmen für Werbezwecke verkauft werden.		X	Stammdaten dürfen nicht an andere Unternehmen weitergegeben werden.
Stammdaten dürfen auch nach Auflösung eines Vertrages verwendet werden, um Werbung zu versenden.		X	Stammdaten dürfen nach der Auflösung eines Vertrages nicht weiter verwendet werden.
Stammdaten dürfen bei Notfällen an Notrufdienste weitergegeben werden.	X		
Stammdaten dürfen für die Erstellung einer Rechnung verwendet werden.	X		
Telekommunikationsanbieter dürfen Stamm- und Standortdaten nur an Notrufdienste weitergeben, nachdem sie eine schriftliche Dokumentation der Notwendigkeit dieser Weitergabe erhalten haben.		X	Telekommunikationsanbieter müssen Stamm- und Standortdaten an Notrufdienste weitergeben. Eine schriftliche Dokumentation der Notwendigkeit muss der Notrufdienst innerhalb von 24 Stunden nachreichen.
Verkehrsdaten dürfen für Verrechnungszwecke gespeichert werden.	X		
Verkehrsdaten müssen ausnahmslos nach drei Monaten gelöscht werden.		X	Solange Rechnungen offen sind, müssen die entsprechenden Verkehrsdaten nicht gelöscht werden.
Kann ein Unglück nur verhindert werden, weil man die Inhaltsdaten einer bestimmten Person bzw. eines Telefons kennt, so dürfen diese Daten an Notrufdienste weitergegeben werden.		X	Nachdem Inhaltsdaten nicht gespeichert werden dürfen, können sie auch nicht an Notrufdienste weitergegeben werden.

FORUM MOBILKOMMUNIKATION

Free access?

	true	false	correct statement
If an emergency service receives an emergency call, the location data of the phone from which the call was made always must be advised immediately thereafter.		X	The location data must be advised if the caller can not tell and the data are necessary to ensure help.
Content data may be stored for accounting purposes.		X	Content data must not be saved.
Content data may be stored only if they are a material component of a communication service.	X		
If an accident can be prevented only because the location data of a certain person and/or of his/her phone are known, such data may be passed on to emergency services.	X		
Master data may be sold to other enterprises for advertising purposes.		X	Master data must not be sold to other enterprises.
Master data may be used also after termination of a contract in order to send advertisements.		X	Master data must not be used after termination of a contract in order to send advertisements.
In emergency cases master data may be passed on to emergency services.	X		
Master data may be used to prepare a bill.	X		
Telecommunications providers may pass on master data and location data only to emergency services after they have received a written documentation of the necessity of such a transfer.		X	Telecommunications providers may pass on master data and location data to emergency services. A written documentation of the necessity must be supplemented within twenty-four hours.
Traffic data may be stored for accounting purposes.	X		
Traffic data must be deleted after three months, even if bills are still outstanding.		X	If bills are outstanding, traffic data concerning these bills, can be stored.
If an accident can be prevented only because the content data of a certain person and/or of a phone are known, such data may be passed on to emergency services.		X	Even if an accident can be prevented only because the content data of a certain person and/or of a phone are known, such data must not be passed on to emergency services.

Smart & Safe

FORUM MOBILKOMMUNIKATION

Big Brother?

Mit 1. April 2012 ist in Österreich die Vorratsdatenspeicherung in Kraft getreten. Anbieter öffentlicher Kommunikationsdienste müssen nun bestimmte Daten, die im Zuge der Handy-, Festnetztelefon-, E-Mail- und Internetnutzung ihrer Kunden anfallen, für die Zeitspanne von sechs Monaten speichern. Die Speicherung soll zur Ermittlung, Feststellung und Verfolgung von Straftaten, die mit mehr als einem Jahr Freiheitsstrafe bedroht sind, erfolgen.
Zur Abfrage von Stammdaten reicht ein begründetes Ersuchen von Staatsanwaltschaft oder Kriminalpolizei, zu dem jeweils ein unabhängiger Staatsanwalt seine Zustimmung geben muss. Für den Zugriff auf Verkehrsdaten brauchen Justiz und Polizei grundsätzlich eine richterliche Genehmigung. In akuten Gefahrensituationen kann diese allerdings auch entfallen. Jede Vorratsdatenabfrage muss einem Rechtsschutzbeauftragten berichtet werden.

Folgende Daten müssen Mobilfunkbetreiber seit 1. April 2012 für sechs Monate speichern:

- Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses
- bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird
- Name und Anschrift des anrufenden und des angerufenen Teilnehmers
- Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone
- die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatz-, Mitteilungs- und Multimediadienste)
- die internationale Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses
- die internationale Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses
- Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an der der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt
- die Standortkennung (Cell-ID) bei Beginn einer Verbindung

Der Inhalt von Gesprächen und Nachrichten sowie Daten über im Internet aufgerufene Adressen dürfen nach wie vor nicht gespeichert werden.

Alles klar? Dann sollte es dir einfach fallen, die nachfolgenden Fragen richtig zu beantworten!

1. *Welche Daten werden im Rahmen der Vorratsdatenspeicherung gespeichert?*

   ❒ Inhaltsdaten ❒ Stammdaten ❒ Standortdaten ❒ Verkehrsdaten

2. *Wie lange müssen die Daten gespeichert werden?*

   .....

3. *Wie lange dürfen die Daten gespeichert werden?*

   .....

4. *Warum werden die Daten gespeichert?*

   .....

5. *Wie soll sichergestellt werden, dass die Vorratsdaten nicht missbräuchlich verwendet werden?*

   .....

   .....

Big Brother?

On 1 April 2012 retention of data became the law in Austria. Providers of public communications services now have to store certain data generated when their customers use mobile phones, land-line phones, e-mail and the internet for a period of six months.
Storage of such data serves the exclusive purpose of investigating, ascertaining and prosecuting crimes that are subject to punishment by imprisonment for more than one year.
A reasoned request by the public prosecutor or by the criminal police is sufficient for an inquiry of master data; an independent public prosecutor must give his consent to such a request. Justice and the police in principle need the approval of a court to access traffic data. In cases of imminent danger such approval need not be obtained. Every inquiry of retained data must be reported to a person responsible for legal protection.

Since 1 April 2012 mobile radio providers must store the following data for six months:

- subscriber number or other ID of the calling terminal and of the called terminal.
- in the case of additional services such as call forwarding or call redirection the subscriber number to which the call is forwarded/redirected.
- name and address of the caller and of the person called.
- date, time of commencement and duration of a communication stating the underlying time zone.
- the nature of the service used (calls, additional services, messaging services and multimedia services).
- International Mobile Subscriber Identity (IMSI) of the calling terminal and of the called terminal.
- International Mobile Equipment Identity (IMEI) of the calling terminal and of the called terminal.
- date and time of first activation of the service and the location ID (cell ID) at which the service was activated, if pre-paid anonymous services are concerned.
- the location ID (cell ID) at the beginning of a connection.

The contents of calls and messages as well as data on addresses visited on the internet still must not be stored.

1. *Which data is stored within the scope of retention of data?*

   ❒ Content data ❒ Master data ❒ Location data ❒ Traffic data

2. *For how long must such data be stored?*

   .....

3. *For how long may such data be stored?*

   .....

4. *Why is such data stored?*

   .....

5. *How can it be ensured that retained data is not misused?*

   .....

   .....

Words to help you:

retention of data – *Vorratsdatenspeicherung* | to ascertain – *ermitteln* | to prosecute – *gerichtlich verfolgen* | public prosecutor – *Staatsawalt* | consent – *Zustimmung* | approval of court – *richterliche Zustimmung* | legal protection – *Rechtsschutz* | subscriber number – *Teilnehmernummer* | call forwarding – *Rufweiterleitung* | call redirection – *Rufumleitung* | commencement – *Beginn*

Pro & Kontra

Sammle Argumente für und gegen die Vorratsdatenspeicherung:
Welche Vorteile bringt sie, welche Nachteile können daraus entstehen?

+	-

Pros & Cons

Collect arguments in favour of and against the retention of data: what are the advantages, what disadvantages may arise?

+	-

Was man über die Vorratsdatenspeicherung wissen muss

Frage: Was verbirgt sich hinter der Vorratsdatenspeicherung?

Antwort: Seit April müssen Anbieter von Telekomdiensten die Kommunikationsdaten ihrer Kunden für mindestens ein halbes Jahr speichern - ob diese nun per Festnetz und Handy telefonieren, E-Mails und SMS verschicken oder im Internet surfen.

Frage: Wer interessiert sich für diese Informationen?

Antwort: Justiz und Polizei wollen auf diese Daten zwecks Verbrechensbekämpfung zugreifen. Die Staatsanwaltschaft braucht dafür eine richterliche Genehmigung, überdies muss die verdächtigte Tat mit mehr als einem Jahr Gefängnis bedroht sein. Die Polizei kann in akuten Situationen - etwa Gefahr für Leib und Leben - aber auch ohne Sanktus eines Richters Auskünfte von den Telekomfirmen verlangen. Jede Abfrage muss einem Rechtsschutzbeauftragten berichtet werden.

Frage: Was lässt sich aus den Datensätzen herauslesen?

Antwort: Wer mit wem wann wie lange telefoniert hat - und auch wo, zumal sich Handys ja immer in eine lokale Funkzelle einwählen. Das Gleiche gilt für verschickte SMS, MMS und E-Mails. Ebenso lässt sich eruieren, wann und wie lange sich ein bestimmter User ins Internet eingewählt hat.

Frage: Werden Inhalte von Gesprächen und Nachrichten gespeichert?

Antwort: Nein. Die Ermittler können höchstens von Absender und Empfänger auf etwaige Inhalte rückschließen.

Frage: Warum halten Datenschützer die Speicherung dann für bedenklich?

Antwort: Weil unbescholtene Bürger unter „Generalverdacht" geraten könnten, fürchtet Hans Zeger von der Arge Daten und nennt ein (fiktives) Beispiel: Bei einem Fußballspiel kommt es zu Ausschreitungen. Also lässt die Polizei ausheben, wer zu dieser Zeit aller im Stadion telefoniert hat. Unbeteiligte mit dem Pech, zur falschen Zeit am falschen Ort zu sein, könnten da rasch in Rechtfertigungsnotstand kommen, nur weil sie einem Freund den Zwischenstand durchgegeben haben, fürchtet Zeger - und der Gegenbeweis, mit Randale nichts zu tun zu haben, sei möglicherweise nicht immer so leicht zu erbringen.

Frage: Wird gespeichert, welche Seiten ein User im Internet besucht hat?

Antwort: Ebenfalls nein. Auch hier gilt das Tabu für Inhalte. Sehr wohl erfasst wird aber die IP- Adresse, unter der sich ein Computer - und damit ein mitunter zuordenbarer Benützer - ins Internet einklinkt. Wieder ein Beispiel von der Arge Daten: Die Polizei sucht den Urheber einer Drohbotschaft, die von einer bestimmten IP-Adresse ausgeschickt wurde. Weil ein und dieselbe öffentliche IP-Adresse aber binnen weniger Minuten mehreren tausend Leuten zugewiesen werde, könnten ebenso viele ins Visier der Ermittler geraten, warnt Zeger.

Frage: Können Internetbenutzer den neugierigen Behörden ein Schnippchen schlagen?

Antwort: Relativ einfach, sagen Fachkundige. Wer anonym surfen will, kann seinen Internetverkehr etwa dank Gratissoftware „Tor" auf schwer nachvollziehbarer Umwege über verschiedene Server schicken - auch für Smartphones gibt es eine entsprechende Version. Die Profiverbrecher und Terroristen, gegen die sich die Überwachungsmethoden richteten, könnten diese in der Regel leicht umgehen, sagt Georg Markus Kainz vom Verein Quintessenz, der sich für Bürgerrechte im Infozeitalter einsetzt: „Das ist wie der Einbrecher, der sich Handschuhe anzieht, um Fingerabdrücke zu vermeiden."

Frage: Wie lassen sich „speicherungssichere" E-Mails verschicken?

Antwort: Indem man einen der Dienste eines kleinen Providers nutzt. Zur Speicherung der E-Mail-Daten sind nämlich nur Anbieter verpflichtet, deren Jahresumsatz 277.000 Euro übersteigt - laut Arge Daten falle gerade die Hälfte der rund 300 Provider unter das Vorratsdaten-Gebot. E-Mails, die vom eigenen Server eines Unternehmens geschickt werden, sind ebenfalls nicht betroffen; allerdings können die Kommunikationsdaten sehr wohl gesichert werden, wenn der Empfänger eine Adresse bei

einem Provider hat, der unter die Vorratsdatenspeicherung fällt. Eine Möglichkeit sind auch außereuropäische E-Mail-Dienste. Doch Vorsicht: Für diese gilt zwar nicht die Vorratsdatenspeicherung, möglicherweise aber eine nicht minder strenge, nationale Bestimmung des jeweiligen Landes des Anbieters.

Frage: Gibt es auch Ausweichmöglichkeiten beim Telefonieren und SMS-Verschicken?

Antwort: Für Smartphones gibt es Apps wie WhatsAPP, über die sich Nachrichten verschicken lassen, ohne dass Absender und Adressaten gespeichert werden - dafür müssen aber beide Seiten dieses Programm verwenden. Das gleiche gilt für Internet-Telefonate mit VoIP-Anbietern (zum Beispiel Skype), sofern man kein Angebot von einem der großen heimischen Provider nutzt, die unter die Vorratsdatenspeicherung fallen. Die Daten direkter Handytelefonate werden ausnahmslos gespeichert. Mit vertragslosen Wertkartenhandys lässt sich aber die Zuordenbarkeit zu einem konkreten Benutzer verschleiern.

Frage: Warum hat Österreich die Vorratsdatenspeicherung eingeführt, Deutschland aber nicht?

Antwort: Im Prinzip gebietet eine EU-Richtlinie, die 2006 im Geiste der Terrorbekämpfung verabschiedet wurde, sämtlichen EU-Staaten, ein entsprechendes Gesetz auszuarbeiten. Nachdem es im Juli 2010 bereits eine Verurteilung wegen Säumigkeit gesetzt hatte, kam Österreich der Verpflichtung nun nach. Auch Deutschland hatte die Richtlinie bereits umgesetzt, doch vor zwei Jahren hat das Bundesverfassungsgericht die in Paragrafen gegossene Regelung aufgehoben. Die EU-Kommission droht nun mit einer Klage beim Europäischen Gerichtshof wegen Verletzung der EU-Verträge - im Extremfall könnte Deutschland eine Strafe in Millionenhöhe ausfassen. Heimische Gegner der Vorratsdatenspeicherung wollen sich am großen Nachbarland hingegen ein Beispiel nehmen: Die Initiative „AK Vorrat" bereitet eine Verfassungsklage vor, zumal das neue Gesetz das Grundrecht auf Privatsphäre verletze.

(Gerald John, DER STANDARD, 3.4.2012)

http://derstandard.at/1333185073067/Der-Staat-speichert-mit-Was-man-ueber-die-Vorratsdatenspeicherung-wissen-muss

So funktioniert die Vorratsdatenspeicherung

Seit 1. April ist die Vorratsdatenspeicherung (VDS) in Österreich in Kraft. Das Thema ist aktuell in aller Munde, doch nicht jeder weiß, was das genau bedeutet. Um Licht ins Dunkel zu bringen, haben wir die wichtigsten Fragen für Sie zusammengestellt und beantwortet.

Befürworter und Kritiker

Laut dem Gesetzgeber ist die VDS ein wichtiges Instrument im Kampf gegen den Terrorismus und die Verbrechensbekämpfung im Allgemeinen. Sie musste aufgrund einer EU-Richtlinie auch in Österreich eingeführt werden. Kritiker sehen das anders. Sie sind davon überzeugt, dass die VDS ein Verstoß gegen das Menschenrecht auf Achtung von Privat- und Familienleben und ein massiver Einschnitt in die Freiheit jedes und jeder Einzelnen sei. Damit würden alle TeilnehmerInnen der Kommunikationsnetze unter einen Generalverdacht gestellt.

Was geschieht bei der Vorratsdatenspeicherung?

Das Gesetz gibt vor, dass alle Kommunikationsdaten wie Telefongespräche, E-Mails, SMS und Co. für sechs Monate gespeichert werden. Vielen Menschen ist gar nicht bewusst, wie häufig sie an einem normalen Tag Spuren in elektronischen Kommunikationsnetzen hinterlassen.

Was wird genau gespeichert?

Bei E-Mails: Hier wird eine ganze Reihe an Daten gespeichert: Die Mail-Adressen der Absender bzw. Empfänger sowie jene IP-Adresse, die für das Routing der E-Mail zuletzt verwendet wurde. Außerdem muss der Zeitpunkt der Anmeldung bei einem E-Mail-Dienst sowie die IP-Adresse des „Anmelders" registriert werden. Damit ist sowohl das Login z.B. in Webmail-Portale gemeint als auch einfach der Zugriff auf die Postfächer bzw. -Server. Der Inhalt von Mails darf aber nicht gespeichert werden.

Bei SMS: Bei jeder Textnachricht müssen beide - bzw. bei „Massen-SMS" alle - betroffenen Telefonnummern gespeichert werden, inklusive Name und Anschrift der Teilnehmer und Zeitpunkt der SMS. Gilt natürlich auch für MMS, also Multimedia-Kurznachrichten. Auch hier gilt: Inhalte dürfen nicht gespeichert werden

Beim Internet-Surfen: Wann immer man mit einer IP-Adresse im Web unterwegs ist, hat das Telekom-Unternehmen den Namen, die Anschrift sowie die Teilnehmerkennung zu speichern. Gilt natürlich auch für Chat-Dienste etc. Vor allem, wenn der User. eine sogenannte dynamische IP-Adresse hat, stellt das einiges an Speicheraufwand dar: Dynamisch sind IP-Adressen, wenn Provider ihren Kunden wechselnde Adressen zuweisen. Das Gegenteil wäre eine sogenannte statische IP-Adresse, die immer dem gleichen User zuordenbar ist.

Ausdrücklich nicht gespeichert werden die Web-Adressen („URLs"), die man ansurft, da die Vorratsdatenspeicherung ja generell keine Inhalte berücksichtigen darf. Allerdings: Auf jenen Servern, deren Sites der Nutzer besuchte, wird die IP-Adresse gespeichert. Und wenn die Behörden diese Server sozusagen ausheben, ist die IP-Adresse künftig eindeutig der Teilnehmerkennung zuzuordnen.

Beim Telefonieren: Egal ob via Handy oder Festnetz - gespeichert werden die betreffende Telefonnummer, Name und Anschrift der Teilnehmer, Datum, Uhrzeit und Dauer des Telefonats. Bei Handys (gilt auch für SMS) werden überdies internationale Geräte- und Teilnehmerkennungen (IMEI/IMSI) erfasst. Bei Anrufweiterleitungen wird natürlich auch jene Nummer, bei der der Anruf schließlich landet, registriert. Gesprächsinhalte dürfen nicht gespeichert werden.

Beim Internet-Telefonieren: Wer glaubt, der Datenspeicherung bei Telefonaten ausweichen zu können, indem sie z.B. Skype oder andere sogenannte „Voice over Internet Protocol"-Dienste (VoIP) verwendet, hat die Rechnung ohne den Gesetzgeber gemacht. Die oben ausgeführten Regeln für Telefonate gelten auch für diesen Kommunikationskanal.

Wie sieht die Sache bei Wertkarten-Handys aus?

Hat man kein Vertragshandy, sondern telefoniert mit einer nicht auf seinen Namen registrierten Wertkarte, gelten die Speichervorschriften wie beim normalen Telefonieren, allerdings sind sein Name und seine Anschrift naturgemäß nicht verfügbar. Dafür muss aber der Zeitpunkt der erstmaligen Aktivierung der Wertkarte gespeichert werden sowie an welchem Standort dies passiert ist (Cell-ID).

Wer darf unter welchen Voraussetzungen auf die Daten zugreifen?

Auf all diese genannten Daten können die Ermittlungs-

behörden grundsätzlich zugreifen. Für das Ausheben von Stammdaten genügt hier ein begründetes Ersuchen seitens der Staatsanwaltschaft bzw. der Kriminalpolizei. Für den Zugriff auf sogenannte Zugangsdaten - also eine Telefonnummer oder eine IP-Adresse - reicht ebenfalls eine schriftliche und begründete Anordnung der Staatsanwaltschaft aus, wobei bei allen solchen Anordnungen das Vier-Augen-Prinzip gilt, also ein zweiter Staatsanwalt das Informationsbegehr absegnen muss.

Für Verkehrsdaten - sie geben Aufschluss über die Kommunikationsvorgänge selbst, also z.B. wer mit wem wie geredet bzw. gemailt hat - muss die Anordnung der Staatsanwaltschaft von einem Richter genehmigt werden. Weitere Voraussetzungen sind der Verdacht eines vorsätzlich begangenen Delikts, das mit einer Strafe von mehr als einem Jahr geahndet wird. Zusätzlich wird zur Kontrolle der Rechtsschutzbeauftragte eingeschaltet.

Wie schützt man sich vor der totalen Überwachung?
Wer nicht will, dass seine Daten gespeichert werden, muss eigentlich auf Telefon, Internet und Co. verzichten. Dies wird heutzutage aber kaum möglich sein. Wenn man einige Tipps beachtet, wird die totale Überwachung etwas abgefedert. Die wirkungsvollste Gegenmaßnahme ist, nicht alle Dienste von einem Anbieter zu beziehen. Insbesondere sollte man Handy, E-Mail-Dienst und Internetzugang trennen. Die E-Mail-Überwachung lässt sich am besten mit Hilfe eines eigenen Mailservers oder verschiedener Anonymisierungsdienste verringern. Letztere gibt es auch kostenlos. Aber Handy und Telefon - die klassischen Überwachungsziele der Behörden - lassen sich leider kaum verstecken.

www.oe24.at/digital/So-funktioniert-die-Vorratsdatenspeicherung/61546846

Vorratsdaten ab 1. April in Kraft: So viel wird gespeichert

Trotz zahlreicher Proteste tritt am 1. April die heftig umstrittene Vorratsdatenspeicherung in Kraft. Damit sind Netzbetreiber dazu verpflichtet, sechs Monate lang sämtliche Telefon- und Internetverbindungsdaten zu speichern und im Zuge der Terrorismus- bzw. Verbrechensbekämpfung auf gerichtliche Anordnung zu übermitteln - mit weitreichenden Konsequenzen für unser aller Privatleben.

Unter die neue Regelung fallen neben den Stammdaten (Name und Adresse des Benutzers) unter anderem Handy- und Telefonnummern, IP- Adressen - also jene Nummer, mit der sich ein Computer ins Internet einklinkt - und E- Mail- Adressen, aber auch die Geräte- Identifikationsnummern von Mobiltelefonen oder die Standortdaten, also wo sich ein Handy zu einem bestimmten Zeitpunkt befindet.

Datenfreigabe nur gegen Ersuchen

Auf all diese Daten können die Ermittlungsbehörden grundsätzlich zugreifen. Für das Ausheben von Stammdaten genügt hier ein begründetes Ersuchen seitens der Staatsanwaltschaft bzw. der Kriminalpolizei. Für den Zugriff auf sogenannte Zugangsdaten - also eine Telefonnummer oder eine IP- Adresse - reicht ebenfalls eine schriftliche und begründete Anordnung der Staatsanwaltschaft aus, wobei bei allen solchen Anordnungen das Vier- Augen- Prinzip gilt, also ein zweiter Staatsanwalt das Informationsbegehr absegnen muss.

Für Verkehrsdaten - sie geben Aufschluss über die Kommunikationsvorgänge selbst, also zum Beispiel wer mit wem wie geredet bzw. gemailt hat - muss die Anordnung der Staatsanwaltschaft von einem Richter genehmigt werden. Eine weitere Voraussetzung ist der Verdacht auf ein vorsätzlich begangenes Delikt, das mit einer Strafe von mehr als einem Jahr geahndet wird. Zusätzlich wird zur Kontrolle der Rechtsschutzbeauftragte eingeschaltet.

Betroffene sollen über Datenzugriff informiert werden

In puncto Rechtsschutz sollen Betroffene grundsätzlich informiert werden, wenn auf ihre Daten zugegriffen wird - zumindest nachträglich (falls Gefahr in Verzug), zuständig dafür sind die Sicherheitsbehörden. Allerdings unterliegt diese Informationspflicht Einschränkungen, so dürfen etwa Ermittlungserfolge nicht gefährdet werden. Jedenfalls ist der Rechtsschutzbeauftragte einzuschalten. Die unzulässige Veröffentlichung von Informationen aus Vorratsdaten wird mit einer Freiheitsstrafe von bis zu einem Jahr geahndet.

So viele unserer Daten werden nun gesammelt

Vielen Menschen ist allerdings nach wie vor nicht bewusst, wie häufig sie an einem ganz normalen Tag Spuren in elektronischen Kommunikationsnetzen hinterlassen. Die folgenden Fallbeispiele fiktiver Nutzer zeigen, wie weitreichend die Konsequenzen der nun in Österreich startenden Überwachung sind.

E- Mails:

Herr A. loggt sich in seinen Computer ein, checkt seine E- Mails und schreibt selbst ein paar. Diese Nachrichten werden über Postserver des Betreibers zugestellt bzw. verschickt. Gespeichert wird dabei einiges: Nämlich die E- Mail- Adresse von Herrn A., die Mailadressen der Absender bzw. Empfänger sowie jene IP- Adresse, die für das Routing der E- Mails zuletzt verwendet wurde.
Außerdem muss der Zeitpunkt der Anmeldung bei einem E- Mail- Dienst sowie die IP- Adresse des „Anmelders" registriert werden. Damit ist sowohl das Login z.B. in Webmail- Portale gemeint als auch der Zugriff auf die Postfächer bzw. -Server. Der Inhalt von Mails darf nicht gespeichert werden.

Die Provider müssen sogar Spam- Mails berücksichtigen. Wenn diese im Postfach der einzelnen User landen, gelten sie als normale Mails und sind der Vorratsdatenspeicherung unterworfen. Nur wenn die Betreiber auf ihren Server wirksame Spam- Filter errichten und die User die Werbemails gar nicht erst zu Gesicht bekommen, dürfen sie ignoriert werden.

SMS:

Teenager B. kommuniziert mit seinen Freunden vornehmlich via SMS. Für seinen Handy- Provider ist einiges zu speichern: Bei jeder Textnachricht müssen beide - bzw. bei „Massen- SMS" alle - betroffenen Telefonnummern gespeichert werden, inklusive Name und Anschrift der Teilnehmer und Zeitpunkt der SMS. Das gilt natürlich auch für MMS, also Multimedia- Kurznachrichten. Auch hier gilt: Inhalte dürfen nicht gespeichert werden.

Internet:
Frau C. recherchiert im Internet. Von ihrem Provider wird ihr eine IP- Adresse zugeteilt, mittels derer sie im Netz verbunden ist. Wann immer sie mit dieser Adresse im Web unterwegs ist, hat das Telekom- Unternehmen ihren Namen, ihre Anschrift sowie die Teilnehmerkennung zu speichern. Das gilt natürlich auch für Chat- Dienste etc. Vor allem, wenn Frau C. eine sogenannte dynamische IP- Adresse hat, stellt das einiges an Speicheraufwand dar: Dynamisch sind IP- Adressen, wenn Provider ihren Kunden wechselnde Adressen zuweisen. Das Gegenstück wäre eine sogenannte statische IP- Adresse, die immer dem gleichen User zuordenbar ist.
Ausdrücklich nicht gespeichert werden die Web- Adressen, die Frau C. ansurft, da die Vorratsdatenspeicherung ja generell keine Inhalte berücksichtigen darf. Allerdings: Auf jenen Servern, deren Sites Frau C. besucht, wird ihre IP- Adresse gespeichert. Und wenn die Behörden diese Server sozusagen ausheben, ist ihre IP- Adresse künftig eindeutig ihrer Teilnehmerkennung zuzuordnen.

Telefon:
Frau D. telefoniert mit ihrem Arbeitgeber - egal ob via Handy oder Festnetz. Gespeichert werden die betreffende Telefonnummer, Name und Anschrift der Teilnehmer, Datum, Uhrzeit und Dauer des Telefonats. Bei Handys (gilt auch für SMS) werden überdies internationale Geräte- und Teilnehmerkennungen (IMEI/IMSI) erfasst. Bei Anrufweiterleitungen wird natürlich auch jene Nummer, bei der der Anruf schließlich landet, registriert. Gesprächsinhalte dürfen nicht gespeichert werden.

Wertkartenhandy:
Herr E. hat kein Vertragshandy, sondern telefoniert mit einer nicht auf seinen Namen registrierten Wertkarte. Es gelten die Speichervorschriften wie oben, allerdings sind sein Name und seine Anschrift naturgemäß nicht verfügbar. Dafür muss aber der Zeitpunkt der erstmaligen Aktivierung der Wertkarte gespeichert werden sowie, an welchem Standort dies passiert ist (Cell- ID).

Internettelefonie:
Frau F. glaubt, der Datenspeicherung bei Telefonaten ausweichen zu können, indem sie z.B. Skype oder andere sogenannte „Voice over Internet Protocol"- Dienste (VoIP) verwendet. Aber sie täuscht sich: Die oben ausgeführten Regeln für Telefonate gelten auch für diesen Kommunikationskanal.

Provider:
Nicht alle österreichischen Provider müssen sich an das Gesetz für die Vorratsdatenspeicherung halten. Für sehr kleine Anbieter wäre die Verpflichtung nicht wirklich verhältnismäßig, wird argumentiert. Und auch private Betreiber sind ausgenommen - also zum Beispiel User, die einen eigenen kleinen Mailserver aufgesetzt haben. Als „Private" gelten überdies Universitäten und ihre Netzwerke.

www.krone.at/Digital/Vorratsdaten_ab_1._April_in_Kraft_So_viel_wird_gespeichert-Glaeserne_Buerger-Story-316560

Vorratsdatenspeicherung: Ab Sonntag bleiben alle Daten gespeichert

Ab 1. April werden Verbindungsdaten von Telefon, Internet und eMail 6 Monate gespeichert.
Wer ab Sonntag mit dem Festnetz- oder Mobiltelefon oder über Internet-Telefoniedienste telefoniert, SMS oder eMails versendet oder im Internet surft, muss damit rechnen, dass österreichische Ermittlungsbehörden sechs Monate lang auf diese Verbindungsdaten zugreifen können. Denn ab 1. April müssen heimische Internet- und Telefonieanbieter sämtliche Verbindungsdaten von Telefon, Handy, Internet und eMail für ein halbes Jahr lang speichern. Polizei und Justiz können dann anhand der verdachtslos gespeicherten Daten feststellen, wer wann mit wem wo telefoniert hat, wer sich wann mit dem Internet verbunden hat und wer wann wem eine eMail oder eine SMS geschickt hat. Kommunikationsinhalte dürfen nicht gespeichert werden.
Datenschützer und Bürgerrechtler sprechen von einem schwerwiegenden Grundrechtseingriff und vom Ende der Unschuldsvermutung. Polizei und Justiz bezeichnen die gespeicherten Daten als „essenziell" für ihre Ermittlungen. Vorgeschrieben wird die verdachtsunabhängige Datenspeicherung durch eine 2006 unter dem Eindruck der Terroranschläge von London und Madrid verabschiedete EU-Richtlinie. In Österreich wurde die Umsetzung der Richtlinie erst beschlossen, nachdem bereits Strafzahlungen der EU drohten.

Viele Ausnahmen

Grundsätzlich gilt, dass auf die Daten „zur Ermittlung, Feststellung und Verfolgung" von Straftaten, die „mit mehr als einjähriger Freiheitsstrafe" bedroht sind, zugegriffen werden darf. Darunter fallen neben Mord und Totschlag auch vergleichsweise geringe Vergehen wie Bigamie. Voraussetzung für den Zugriff auf die Daten ist eine gerichtlich bewilligte Anordnung der Staatsanwaltschaft. Allerdings gibt es zahlreiche Ausnahmen.
Für den Zugriff der Ermittler auf IP-Adressen (jene Nummer, mit der sich ein Computer ins Internet einklinkt) und eMail-Daten gibt es etwa keine Strafschwelle. Auch eine richterliche Bewilligung ist nicht vorgesehen. Bei der im Sicherheitspolizeigesetz (SPG) geregelten Gefahrenabwehr muss für den Zugriff auf Standortdaten im Mobilfunk und IP-Adressen ebenfalls kein Richter eingeschaltet werden. [...]

Aufwand für Internetanbieter

Ein Großteil der Daten wurde von den Betreibern, die sie etwa für Verrechnungszwecke brauchten, auch schon bisher gespeichert. Allerdings mussten sie gelöscht werden, wenn sie für den Betrieb nicht mehr benötigt wurden. Nun müssen sie getrennt als Vorratsdaten gespeichert werden. Telefoniedaten werden in der Regel nach drei Monaten zu Vorratsdaten. Bei Internet-Verbindungsdaten ist dies je nach Betreiber unterschiedlich. eMail-Daten wurden bisher überhaupt nicht gespeichert, da sie für die Geschäftsmodelle der Betreiber irrelevant sind.
Die Kosten für den Aufbau der Infrastruktur für die Vorratsdatenspeicherung werden auf 15 bis 20 Millionen geschätzt. Internet-Anbieter müssen ihre Systeme anpassen und da die Daten bei ihnen gespeichert werden auch ihre Speicherkapazitäten erweitern. 80 Prozent der Kosten werden vom Bund getragen. 20 Prozent bleiben bei den Anbietern hängen. Zahlen werden also letztlich die österreichischen Bürger als Steuerzahler und Kunden.
EU prüft. In der EU wird die Vorratsdatenspeicherung gerade geprüft. Ein im vergangenen April veröffentlichter Evaluationsbericht spricht von gravierenden Mängeln bei der Umsetzung. In einigen Mitgliedsstaaten, darunter auch Deutschland, wurde die Datenspeicherung vom Verfassungsgericht gestoppt. Auch der Europäische Gerichtshof (EuGH) prüft auf Antrag Irlands, ob die Richtlinie mit der europäischen Grundrechtecharta vereinbar ist. Im Juli will EU-Innenkommissarin Cecilia Malmström einen überarbeiteten Entwurf der Richtlinie vorstellen.

http://kurier.at/techno/4490618-vorratsdatenspeicherung-ab-sonntag-bleiben-alle-daten-gespeichert.php

Vorratsdatenspeicherung startet mit Aprilscherz

Wien. Die Vorratsdatenspeicherung ist in Österreich in Kraft. Die ab sofort für Provider verpflichtende Speicherung sämtlicher Kommunikationsdaten von Telefon, Handy, E-Mail und Internetdiensten für sechs Monate soll der Terror-Bekämpfung dienen. Kritiker befürchten aber massive Eingriffe in die Privatsphäre. Erst am Samstag versammelten sich in Wien und anderen Landeshauptstädten Hunderte Menschen zu Protesten gegen die Richtlinie. AnonAustria, der österreichische Ableger des Hackerkollektivs Anonymous, verkündete zudem, über 10.295 Politiker-E-Mails zu verfügen - ein Aprilscherz, wie sich herausstellen sollte.

Ab Mitternacht wollte AnonAustria die Mails unter dem Codenamen „Operation Pitdog" schrittweise veröffentlichen - und machte in einer Pressemitteilung klar, damit Österreich „erschüttern" zu wollen. Wie sich in der Nacht auf Sonntag herausstellte, handelte es sich bei diesen vermeintlichen Leaks jedoch um einen Aprilscherz: Die Mails existierten schlichtweg nicht.

In einer Stellungnahme schrieb das Hackerkollektiv: „Die Leaks waren komplett frei erfunden um die Media attention für die VDS (Vorratsdatenspeicherung, Anm.) so weit wie es geht hochzukurbeln. Dies war auch ein voller Erfolg." Dass diese Aktion allerdings innerhalb des Kollektivs nicht ganz unumstritten waren, räumt AnonAustria ein. In der Stellungnahme war die Rede von „internen Differenzen". Immerhin aber will man mit der Aktion erreicht haben, Politiker eine Lehre erteilt zu haben, „wie es sich anfühlt wenn jemand Daten über einen hat die nicht für die Öffentlichkeit gemacht sind."
Auf Twitter stieß der Aprilscherz auf geteilte Meinungen. „Das war...dumm", ist hier ebenso zu lesen wie Glückwünsche zum „erfolgreichen Aprilscherz". Zusatz: „Nur glauben wird euch keiner mehr was."

Initiative mit zehntausenden Unterstützern
Ungeachtet der Verwirrung, die AnonAustria mit dieser Aktion gestiftet hat, formiert sich auch an anderen Fronten der Widerstand gegen die in Kraft getretene Vorratsdatenspeicherung. Die Initiative Arbeitskreis Vorrat („AK Vorrat") gibt auf ihrer Webseite an, bereits über 85.000 Untersützungserklärungen erhalten zu haben, um gegen die Vorratsdatenspeicherung vorzugehen. Konkret werden dabei Klagen vor dem Verfassungsgerichtshof ins Auge gefasst. Bereits am Freitag hatten die Grünen erklärt, diese Initiative unterstützen zu wollen.
Auch die FPÖ hatte vergangene Woche angekündigt, eine Verfassungsbeschwerde gegen das Gesetz zur Vorratsdatenspeicherung einzubringen. „Wir wollen den Verfassungsgerichtshof einladen, sich das Gesetz anzuschauen und wieder außer Kraft zu setzen. Datenschutz muss über allem stehen", sagte FPK-Landeshauptmann Gerhard Dörfler.

Ob der Weg vor den Verfassungsgerichtshof die Vorratsdatenspeicherung aushebeln kann, ist freilich fraglich. Die Richtlinie basiert auf einer EU-Verordnung aus dem Jahr 2006, deren Einführung Österreich - neben anderen Ländern - lange hinauszögerte. Deutschland etwa riskiert mit der verspäteten Umsetzung der Richtlinie eine Klage der EU-Kommission vor dem Europäischen Gerichtshof - die Frist läuft in wenigen Wochen aus.

In Österreich ist es Behörden nun möglich, für einen Zeitraum von sechs Monaten auf sämtliche Kommunikationsdaten zuzugreifen. Zudem würden mit der verpflichtenden Speicherung der Daten auch die Kommunikationsbetreiber über umfangreiche Daten wie Handy- und Telefonnummern, Adressdaten, sowie Geräte-und andere Identifikationsnummern und Informationen zum Nutzungsverhalten verfügen - Datensätze, für die sich am Schwarzmarkt für viel Geld verdienen ließe, befürchten Kritiker Datenlecks bei den Providern.

Immerhin sollen Betroffene grundsätzlich - zumindest nachträglich - informiert werden, wenn Behörden auf ihre Daten zugreifen. Allerdings unterliegt diese Informationspflicht Einschränkungen, so dürfen etwa Ermittlungserfolge nicht gefährdet werden. Jedenfalls ist der Rechtsschutzbeauftragte einzuschalten. Die unzulässige Veröffentlichung von Informationen aus Vorratsdaten wird mit einer Freiheitsstrafe bis zu einem Jahr geahndet.

www.wienerzeitung.at/themen_channel/wz_digital/digital_news/447533_Vorratsdatenspeicherung-startet-mit-Aprilscherz.html

Vorratsdaten: Wer ab 1. April was wann wie wissen darf

Wer mit wem telefoniert und SMS schreibt, wird gespeichert. Polizei und Staatsanwaltschaft dürfen zugreifen. Weitere Antworten zur umstrittenen Vorratsdatenspeicherung, gesammelt von DiePresse.com.

Die Vorratsdatenspeicherung sorgt für Unmut bei Datenschützern. Die Grünen und das BZÖ unterstützen eine Verfassungsklage gegen die Überwachungsmaßnahme. Im Vorfeld der neuen Regelungen gab es aber viele Falschinformationen. DiePresse.com bietet ein Überblick darüber, was ab 1. April wirklich der Fall sein wird.

Warum gibt es die Vorratsdatenspeicherung?

Die Idee, Kommunikations-Verbindungsdaten auf Vorrat zu speichern, war eine Reaktion auf die Terroranschläge vom 11. September 2001 in New York, vom 11. März 2004 in Madrid und vom 13. Juli 2005 in London. Daraus entstand die EU-Richtlinie 2006/24/EG, in der die Speicherung dieser Daten vorgesehen wird. Österreich, genauer Infrastrukturministerin Doris Bures, hat sich bewusst lange Zeit mit der Umsetzung gelassen. Erst als 2010 eine Millionenstrafe wegen Nichtumsetzung der Regeln drohte, wurden die entsprechenden Gesetzesvorlagen eingebracht.

Welche Daten werden gespeichert?

Verbindungs-, Standort- und Nutzer-Daten folgender Kommunikationsmittel werden gespeichert: Telefongespräche, Kurzmitteilungen, Multimedia-Nachrichten (MMS), Internet-Telefonie und die Übertragung von Daten über sämtliche Internet-Protokolle einschließlich E-Mail. Konkret bedeutet das, dass bei Gesprächen etwa die Telefonnummern beider Teilnehmer, Zeitpunkt, Dauer und Standort des Anrufenden gespeichert werden. Bei E-Mails oder beim Surfen im Internet wird die IP-Adresse aufgezeichnet, die in der Regel einem einzelnen Computer zugeordnet werden kann. Im österreichischen Telekommunikationsgesetz (TKG) sind diese Punkte alle genau aufgelistet.

Werden auch Inhalte gespeichert?

Nein. Oft lassen andere Daten aber Rückschlüsse auf den Inhalt zu. Etwa, wenn regelmäßig bei Selbsthilfegruppen, bestimmten Ärzten oder einschlägigen Hotlines angerufen wurde.

Wer hat Zugriff auf Vorratsdaten?

Auf die Vorratsdaten darf in Österreich ab 1. April von zwei Seiten zugegriffen werden. Einerseits durch die Staatsanwaltschaft im Rahmen der Strafverfolgung, was die Strafprozessordnung (StPO) regelt. Und andererseits durch die Sicherheitsbehörden, was durch das Sicherheitspolizeigesetz (SPG) geregelt ist. Für beide gelten aber unterschiedliche Bedingungen, unter denen sie auf die Daten zugreifen dürfen. Die Staatsanwaltschaft benötigt eine richterliche Genehmigung für Standort- und Verbindungsdaten. Für eine IP- und E-Mail-Adressen-Abfrage ist das nicht vorgesehen. Hier reicht eine staatsanwaltliche Anordnung. Es gilt aber das Vier-Augen-Prinzip. Bei der Polizei reicht eine akute Gefährdungssituation als Begründung, um auf Vorratsdaten zuzugreifen. Jegliche Abfrage muss aber genau protokolliert und dem Rechtschutzbeauftragten von Justiz- und Innenministerium bekannt gegeben werden.

Wann wird auf die Daten zugegriffen?

Die Staatsanwaltschaft nutzt Verbindungs- und Standortdaten, um einen Verdacht bei Ermittlungen zu erhärten oder zu entkräften.

Dazu muss aber ein Offizialdelikt mit einer Strafandrohung von mindestens zwei Jahren bestehen. Friedrich König, Leiter der Abteilung Strafverfahrensrecht im Justizministerium, bezeichnet diese Daten als „essenziell" für die Ermittlungen. Die Polizei wiederum nutzt diese Informationen laut Innenministerium in den meisten Fällen nur bei Akutsituationen. In diesem Zusammenhang wird gern das Beispiel einer Entführung gebracht, wo das Opfer durch Handyortung ausfindig gemacht werden kann.

Kamen Behörden schon bisher an die Daten?

Ja. Schon bisher durften Ermittler und Polizei auf Betreiberdaten und Handy-Standortinformationen zugreifen, sofern sie verfügbar waren. Im Wesentlichen ändert sich nur der Zeitraum, der für die Abfrage zur Verfügung steht.

Wie werden die Daten übermittelt?

Für Abfragen der Vorratsdaten gibt es eine sogenannte Durchlaufstelle. Sie ist in Wahrheit auch nur ein Server und ist zentral im Bundesrechenzentrum angesiedelt. Ermittler richten eine Vorratsdatenabfrage an den Provider, dieser übermittelt die gewünschten Informationen ver-

schlüsselt an dieses Gerät, welches die Daten wiederum verschlüsselt an die Ermittler leitet. Sollte diese Schnittstelle einmal ausfallen oder defekt sein, würden die Behörden auf versiegelte Kuverts oder andere nicht so technische Mittel zurückgreifen.

Was kann aus diesen Daten gelesen werden?
2009 hatte der deutsche Politiker Malte Spitz (Grüne) die über ihn gespeicherten Daten bei der Deutschen Telekom beantragt. „Zeit Online" hat die Daten damals ausgewertet. Das Ergebnis: Eine Tabelle mit mehr als 35.000 Verbindungen. Sein Handy meldete sich alle zehn Minuten bei einer Funkzelle an und gab damit seinen ungefähren Standort preis. Seine Bewegungen in dem Zeitraum wurden zu 78 Prozent erfasst. Inhalte, wie Gespräche und Texte, werden nicht gespeichert. Dennoch lässt sich daraus so einiges lesen. Zum Beispiel, wo sich Malte Spitz zum Zeitpunkt einer konkreten Demonstration aufhielt und mit wem er telefonierte. Aus der Häufigkeit und Dauer von Telefonaten mit bestimmten Nummern lassen sich sogar Beziehungen analysieren. Werden die Daten mit Daten anderer Internetdienste verbunden, wird das Bild noch genauer. Infrage kommen insbesondere Twitter, Blogs oder öffentliche Fotonetzwerke wie Flickr. Zudem lassen gesammelte Bewegungsdaten eines halben Jahres Prognosen darüber zu, wohin sich eine Person an einem bestimmten Tag vermutlich bewegen wird.

Erfahren Bürger, ob Daten genutzt wurden?
Die Staatsanwaltschaft ist verpflichtet, Betroffene zu informieren, wenn im Zuge der Ermittlungen auf deren Vorratsdaten zugegriffen wurde. Bei der Polizei sieht es etwas anders aus. Fällt die Datenabfrage in einem Zeitraum, wo Standort- oder Verbindungsdaten bei den Providern noch für betriebliche Zwecke genutzt werden, muss ein Betroffener nicht informiert werden. Erst wenn der Betreiber die Daten nicht mehr benötigt und diese in den Pool der Vorratsdaten wandern, muss eine Information an den jeweiligen Kommunikationsteilnehmer ergehen. Jeder Bürger hat aber das Recht, jederzeit bei den Behörden anzufragen, ob und welche Daten über ihn abgefragt wurden.

Wieviel kostet die Vorratsdatenspeicherung?
In Österreich wurden die Kosten für die Anpassung von Technik und den betrieblichen Abläufen zur Datenarchivierung und Bearbeitung von Anfragen auf insgesamt 15 Millionen Euro geschätzt. 20 Prozent davon, also drei Millionen Euro, sollen von den Unternehmen selbst getragen werden, den Rest übernimmt der Bund. Der Löwenanteil davon (63 Prozent) wird vom Infrastrukturministerium berappt, das Innenministerium zahlt 34 Prozent, das Justizressort einen Fixbetrag von 360.000 Euro, was drei Prozent entsprechen soll. Die EU-Richtlinie verpflichtet die Staaten nicht zur Übernahme der Kosten.

Wie setzen andere Staaten die Richtlinie um?
Neben Österreich haben noch vier weitere Staaten die Richtlinie nicht umgesetzt. In Schweden wird noch am Entwurf für das nationale Gesetz geschmiedet. In Deutschland, Rumänien und der Tschechischen Republik war die Richtlinie bereits umgesetzt, die entsprechenden Gesetze wurden aber von den nationalen Verfassungsgerichten wieder gekippt. Andere Länder, wie etwa Großbritannien und Frankreich, haben die Vorratsdatenspeicherung strenger umgesetzt als Österreich. Dort müssen die Daten nicht nur sechs, sondern zwölf Monate gespeichert werden. Und in Ungarn dürfen Ermittler ohne Angabe von Gründen auf die Informationen zugreifen.

Drohen Sanktionen bei einer Nichtumsetzung?
Deutschland hat es bisher nicht geschafft, seine gekippte Vorratsdatenregelung neu zu gestalten. Die EU-Kommission hat dem Land deshalb jetzt die Rute ins Fenster gestellt. Sollte bis Mitte April keine Lösung gefunden werden, droht eine Klage vor dem Europäischen Gerichtshof. Dieser kann eine Millionenklage gegen ein Land aussprechen, das eine Richtlinie nicht korrekt umsetzt.

Welche Sanktionen drohen den Providern?
Die Provider sind durch das Telekommunikationsgesetz verpflichtet, die Vorratsdatenspeicherung korrekt umzusetzen. Wenn hier Fehler geschehen, oder etwa Daten nicht rechtzeitig wieder gelöscht werden, kann es Verwaltungsstrafen von bis zu 58.000 Euro pro Fall hageln.

Vorratsdatenspeicherung verfassungswidrig?
Diese Frage lässt sich noch nicht beantworten. Die Kärntner Landesregierung will aber die Verfassungsmäßigkeit der österreichischen Regelungen vom Verfassungsgerichtshof prüfen lassen. In Deutschland hat das Bundesverfassungsgericht die dortigen Regeln zur Vorratsdatenspeicherung für grundgesetzwidrig erklärt. Vereinbar ist die Speicherung auf Vorrat nach Ansicht vieler Juristen auch weder mit der EU-Grundrechtecharta von 2009, noch mit der Europäischen Menschenrechtskonvention.

http://diepresse.com/home/techscience/internet/745023/Vorratsdaten_Wer-ab-1-April-was-wann-wie-wissen-darf