

PRIVAT – kein Zutritt?

persönliche Daten

sensible Daten

Identitätsdiebstahl

gläserner Mensch

Privatsphäre

Handyortung

SPAM-SMS

Schadprogramme

Vorratsdatenspeicherung



**persönliche
Daten**



sensible Daten



**Identitäts-
diebstahl**



gläserner Mensch

Privatsphäre

Handyortung



SPAM-SMS



**Schad-
programme**



**Vorratsdaten-
speicherung**

Schon gehört?

Lies die einzelnen Schilderungen durch und versuche anschließend, die jeweils dargestellte Problematik in einem Satz zusammenzufassen.



Paul S. & eine App mit unentdeckten Fähigkeiten

Als ich diese App entdeckt habe, war ich echt begeistert: „Beame mit nur einem Knopfdruck deine privaten Fotos in die Filmsets aktueller Blockbuster!“ Echt lässig! So lässig, dass sich auch alle meine Freunde über eine MMS freuen durften, in der sie an der Seite ihrer persönlichen Leinwandhelden zu bewundern waren. Echt cool! Haben übrigens auch alle meine Freunde gefunden!

Weniger cool war allerdings, dass wir kurze Zeit später mit SPAM-SMS überhäuft wurden. Und dann kam's auch schon in der Zeitung: Die Blockbuster-App konnte nämlich noch einiges mehr als auf Knopfdruck zu beamen. Ohne dass ich es bemerkt habe, hat sie auf meine persönlichen Kontakte und das Anrufverzeichnis zugegriffen. Und das Peinliche daran ist, dass ich dem App-Betreiber beim Installieren der App sogar die Erlaubnis dafür erteilt habe. Jetzt hoffe ich nur, dass nicht noch mehr Überraschungen auf mich warten. Würde mir grad noch fehlen, dass auch noch meine Handyfotos irgendwo im Web auftauchen ...



Sandra T. & verpasste Anrufe, die teuer zu stehen kommen ...

Meine letzte Handyabrechnung hat mich echt geschockt: Normalerweise zahle ich um die 12 Euro im Monat, und diesmal wurden alleine für Anrufe bei Mehrwertnummern mehr als 40 Euro verrechnet! Und das wo ich mir sicher war, keine kostenpflichtigen Nummern angerufen zu haben!

Nach dem ersten Schreck habe ich die Rechnungshotline meines Mobilfunkanbieters angerufen. Und als mich der nette Mann in der Leitung nach Anrufen unbekannter Nummern gefragt hat, war mir dann auch schon alles klar! Vor einiger Zeit hatte ich nämlich jede Menge verpasster Anrufe verschiedener Nummern. Und jedesmal wenn ich versucht habe zurückzurufen, bin ich in seltsamen Tonbandschleifen gelandet. So habe ich, ohne es zu merken, bei kostenpflichtigen Diensten angerufen und meine Telefonrechnung nach oben gekurbelt ...



Isabella F. & die teure Gratis-App

„Drohende Gefahr durch Handy-Hacker“ – bis vor kurzem hab ich mir beim Lesen solcher Schlagzeilen gedacht, dass das ja wohl maßlos übertrieben ist. Seit letzter Woche sehe ich das allerdings ganz anders! Da bin ich nämlich selbst Opfer eines heimtückischen Angriffs durch Handy-Hacker geworden. Gemeinsam mit einer Gratis-App wurde mir – ebenfalls kostenlos, allerdings auch unerwünscht – ein Trojaner mitgeliefert. Und der hat dann, ohne dass ich es bemerkt habe, SMS an alle meine Kontakte verschickt. Erst als mich eine Freundin gefragt hat, warum ich eigentlich

dauernd leere SMS versende, habe ich gecheckt, dass da etwas nicht stimmen kann und meinen Mobilfunkanbieter angerufen. Da hat sich dann herausgestellt, dass von meinem Handy täglich um die 300 SMS versendet wurden ...

.....

.....



Tom K. & der unheimliche Shoppingtrip

Eigentlich hatte ich alles perfekt geplant! Am Montagmorgen war mir einfach ganz furchtbar übel, sodass ich nicht zur Schule gehen konnte. Und nachdem meine Eltern mich gebührend bemitleidet und sich in Richtung Arbeit begeben hatten, habe ich mich dann – unentdeckt von den Nachbarn – aus dem Haus geschlichen, bin zum Bahnhof gedüst und von dort direkt nach Graz weitergefahren: Shoppen statt Schulbank drücken! Während meines kleinen Ausflugs habe ich dann auch immer wieder meinen Status auf Facebook geändert. Mit meinem neuen Smartphone geht

das ja supereasy. Da hat dann eine Statusmeldung à la „Ich fühl mich soooo schlecht“ die nächste gejagt. Grundsätzlich genial! Dumm nur, dass ich vor einiger Zeit bei Facebook die Funktion aktiviert habe, dass bei jeder neuen Statusmeldung mein Aufenthaltsort automatisch ermittelt und im Profil angegeben wird. So konnten meine Eltern auf meinem Facebook-Profil meine Shoppingtour live mitverfolgen ...

.....

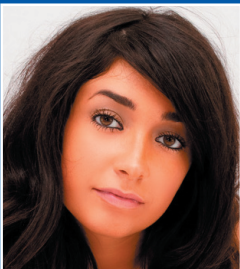
.....



Florian E. & sein zweites Ich

Bis ich das Geld für mein neues Smartphone zusammengespart hatte, hat's eine gefühlte Ewigkeit gedauert. Die letzten Euro kamen dann noch aus der Onlineversteigerung meines alten Handys. Das Glück mit meinem neuen Smartphone hat allerdings nur bis letzten Freitag angehalten. Da hat mich nämlich einer aus der Parallelklasse mächtig dumm angemacht, von wegen: „Du treibst es ja ziemlich bunt, Loverboy2000“. Erst nach langem Hin und Her ist er dann endlich damit herausgerückt, was dieser dumme Spruch sollte. Auf einem bekannten Onlinedating-Portal

gab's seit neuestem ein „Loverboy2000“-Profil. Und dieses Profil war mit privaten Fotos von mir gespickt. Der Käufer meines alten Handys hatte die Bilder offensichtlich entdeckt und es für besonders witzig und originell gehalten, damit „spaßhalber“ ein Profil auf dem Onlineportal anzulegen ...



Zeynep K. & die Abofalle

Mein Klingelton hat mich schon lange genervt. Deswegen war ich auch Feuer und Flamme als ich meinen Lieblingssong als Klingelton gefunden habe. Ging auch ganz easy: Ich hab in der App einfach „Kaufen“ bestätigt, und schon stand mein neuer Klingelton zum Download bereit. So weit, so gut! Das böse Erwachen kam allerdings, als plötzlich das gesamte Guthaben auf meiner Wertkarte aufgebraucht war. Da hat sich dann herausgestellt, dass ich mit meinem Klick auf „Kau-

fen“ nicht nur den einen Klingelton, sondern gleich ein ganzes Klingeltonabo bestellt habe. Ein teurer Spaß ...

Ich und mein Handy



1. Ich bin

☐ männlich

☐ weiblich

2. Hast du ein Telefon, mit dem du ins Internet einsteigen kannst?

☐ Ja

☐ Nein

Wenn Ja:

3. Was tust du, wenn du mit deinem Handy online gehst? Nummeriere die vorgeschlagenen Möglichkeiten von 1 bis 5: „1“ steht für „am häufigsten“, „5“ für „am seltensten“.

☐ ...

Im Internet surfen.

☐ ...

E-Mails versenden und empfangen.

☐ ...

Wetterbericht abrufen.

☐ ...

Mein Profil auf Facebook/Twitter etc. checken.

☐ ...

Ich nutze Routenplaner, z.B. „Quando“ vom VOR.

4. Was machst du mit deinem Handy, wenn du es nicht mehr brauchst?

☐ Ich werfe es weg.

☐ Ich schenke es einem Verwandten/Freund.

☐ Ich spende es. (Z.B. Ö3)

☐ Ich hebe es bei mir zu Hause auf.

☐ Ich verkaufe es.

☐ Ich gebe es zum Recycling.

5. Kontrollierst du, welche Daten noch auf deinem Telefon gespeichert sind, bevor du es ersetzt?

☐ Ja

☐ Nein

6. Ist dein Handy schon einmal verloren gegangen oder gestohlen worden?

☐ Ja

☐ Nein

Falls ja – worüber hast du dich am meisten geärgert, als das Handy weg war?

☐ Dass ich nicht mehr telefonieren konnte.

☐ Dass alle meine Telefonnummern weg waren.

☐ Dass alle meine Fotos weg waren.

☐ Dass ich keine SMS mehr schicken konnte.

☐ Dass ich nicht wusste, wer mein Telefon vielleicht gefunden hatte.

7. Hast du schon einmal Werbe-SMS bekommen, die du nicht haben wolltest?

☐ Ja

☐ Nein

8. Hast du ein Smartphone?

☐ Ja

☐ Nein

9. Kannst du Apps auf deinem Handy installieren?

☐ Ja

☐ Nein

Wenn Ja:

10. Wieviele Apps sind auf deinem Telefon installiert?

☐ keine

☐ 1 bis 5

☐ 6 bis 10

☐ 11 bis 15

☐ mehr als 15

☐ Weiß ich nicht.

Wie viele Prozent dieser Apps nutzt du regelmäßig? %

11. Welche Apps verwendest du am häufigsten? Notiere deine Top 3:

1.

2.

3.

12. Was passiert mit Apps, die du nicht mehr verwendest?

☐ Die bleiben auf meinem Handy.

☐ Die lösche ich wieder.

☐ Ich würde sie gerne löschen, weiß aber nicht wie.

13. Welche Sicherheitsmaßnahmen hast du für den Fall eines Handyverlustes oder -diebstahls getroffen?

☐ Ich sichere meine Daten regelmäßig.

☐ Ich habe auf meinem Handy die Sperre aktiviert.

☐ Ich habe mir die IMEI-Nummer meines Handys notiert.





Ich & mein Handy Auswertungsbogen



1. Befragt wurden

- männlich: in Prozent: %
- weiblich: in Prozent: %

2. Hast du ein Telefon, mit dem du ins Internet einsteigen kannst?

- Ja: in Prozent: %
- Nein: in Prozent: %
- Anteil aller befragten Frauen, die das Internet am Handy nutzen:
..... von insgesamt in Prozent: %
- Anteil aller befragten Männer, die das Internet am Handy nutzen:
..... von insgesamt in Prozent: %

3. Häufigste Tätigkeiten im Internet:

	Anzahl der Stimmen	Platz
Surfen		
E-Mails		
Wetter		
Social Networks		
Routenplaner		

4. Was machst du mit deinem Handy, wenn du es nicht mehr brauchst?

- entsorgen: in Prozent: %
- verschenken: in Prozent: %
- spenden: in Prozent: %
- aufheben: in Prozent: %
- verkaufen: in Prozent: %
- Recycling: in Prozent: %



Smart & Safe



5. Kontrollierst du, welche Daten noch auf deinem Telefon gespeichert sind, bevor du es ersetzt?

- Ja: in Prozent: %
- Nein: in Prozent: %

6. Ist dein Handy schon einmal verloren gegangen oder gestohlen worden?

- Ja: in Prozent: %
- Nein: in Prozent: %

Worüber hast du dich am meisten geärgert, als das Handy weg war?

- Dass ich nicht mehr telefonieren konnte: in Prozent: %
- Dass alle meine Telefonnummern weg waren: in Prozent: %
- Dass meine Fotos weg waren: in Prozent: %
- Dass ich keine SMS verschicken konnte: in Prozent: %
- Dass ich nicht wusste, wer mein Telefon gefunden hatte: in Prozent: %

7. Hast du schon einmal Werbe-SMS bekommen, die du nicht haben wolltest?

- Ja: in Prozent: %
- Nein: in Prozent: %

8. Besitzt du ein Smartphone?

- Ja: in Prozent: %
- Nein: in Prozent: %

- Anteil aller befragten Frauen, ein Smartphone besitzen:

..... von insgesamt in Prozent: %

- Anteil aller befragten Männer, die ein Smartphone besitzen:

..... von insgesamt in Prozent: %

9. Kannst du Apps auf deinem Handy installieren?

- Ja: in Prozent: %
- Nein: in Prozent: %

- Anteil aller befragten Frauen, die ein App-fähiges Handy besitzen:

..... von insgesamt in Prozent: %

- Anteil aller befragten Männer, die ein App-fähiges Handy besitzen:

..... von insgesamt in Prozent: %



10. Wieviele Apps sind auf deinem Handy installiert?

- Keine: in Prozent: %
- 1-5: in Prozent: %
- 6-10: in Prozent: %
- 11-15: in Prozent: %
- Mehr als 15: in Prozent: %
- Weiß ich nicht: in Prozent: %

11. Top 3 der Apps:

Titel der App	Anzahl der Nennungen	Platzierung

12. Was passiert mit Apps, die du nicht mehr verwendest?

- Bleiben auf dem Handy: in Prozent: %
- Werden gelöscht: in Prozent: %
- Würde ich löschen, weiß aber nicht wie: in Prozent: %

13. Welche Sicherheitsmaßnahmen hast du für den Fall eines Handyverlustes oder -diebstahls getroffen?

- regelmäßige Datensicherung: in Prozent: %
- Aktivierung der Handysperre: in Prozent: %
- Notieren der IMEI-Nummer: in Prozent: %



Ich & mein Handy

Zahlen im Vergleich

Die folgenden Ergebnisse stammen, falls nicht anders angegeben, vom Austrian Internet Monitor-Consumer (AIM-C). Der AIM-C wird von INTEGRAL Markt- und Meinungsforschung auf Basis von insgesamt 12.000 telefonischen Interviews pro Jahr (3.000 pro Quartal) und ergänzenden Online-Interviews durchgeführt und ist repräsentativ für die österreichische Bevölkerung ab 14 Jahren. (www.integral.co.at/de/downloads/?f=AIM)

Verfügen Sie über ein internetfähiges Handy?

- 24% aller österreichischen HandybesitzerInnen ab 14 Jahren haben ein internetfähiges Handy.
- 19% aller befragten Frauen nutzen Internet am Handy.
- 30% aller befragten Männer nutzen Internet am Handy.
- 50% aller Befragten im Alter von 14 bis 19 nutzen Internet am Handy. Bei den 30- bis 39-Jährigen sind es 31%, bei den 40- bis 49-Jährigen 25%.

Tätigkeiten im Internet

Tätigkeit	Platz
Surfen	1
Social Network	2
Wetter	3
E-Mails	4
Routenplaner	5

Handyentsorgung

Laut Umfrage des Meinungsforschungsinstituts Aris aus dem November 2011, bei der 1.000 Deutsche über 14 Jahren befragt wurden, **heben** zwei von drei HandybesitzerInnen (**66,67 %**) ihr altes Telefon **auf**, wenn sie ein neues erhalten. Jede dritte Befragte (**33 %**) **verschenkt** ihr Telefon.

Handydiebstahl und -raub

Laut Innenministerium wurden im Jahr 2008 **20.500 Handys** gestohlen, das macht pro Tag mehr als 56 Handydiebstähle. In dieser Zahl sind allerdings nur jene Fälle erfasst, bei denen eine offizielle Diebstahlsanzeige gemacht wurde. Die häufigsten Tatorte sind Gasthäuser, öffentliche Verkehrsmittel, Kaufhäuser und Schulen. Das Delikt des **Handyraubs** wurde im Jahr 2011 **444-mal** verübt – das entspricht im Vergleich zum Vorjahr einer Steigerung von 20%.

Smartphonebesitzer

32% der österreichischen HandybesitzerInnen haben ein Smartphone.
Im Zuge der deutschen JIM Studie wurden im Jahr 2010 1.208 Jugendliche und junge Menschen zwischen 12 und 19 Jahren befragt. Die Studie kam zu folgendem Ergebnis:
14% aller 12- bis 19-Jährigen haben ein Smartphone:

- 11% der Mädchen.
- 16% der Jungen.

Apps am Handy

20% der österreichischen HandybesitzerInnen haben Apps installiert:

- 12% der weiblichen Handybesitzerinnen.
- 28% der männlichen Handybesitzer.

Bei den **14- bis 19-Jährigen** haben **42%** aller HandynutzerInnen Apps installiert.
Bei den 30- bis 39-jährigen sind es 28%, bei den 40- bis 49-Jährigen nur mehr 16%.

Anzahl der Apps

Die durchschnittliche österreichische App-UserIn hat **zehn Apps** auf ihrem Telefon installiert, von denen **sechs regelmäßig verwendet** werden.

Top 3 der Apps

Die beliebtesten Apps der österreichischen App-UserInnen kommen aus den Bereichen:

- Navigation: 72%
- Wetter: 64%
- Spiele: 60%
- Soziale Netzwerke: 57%

Was passiert mit Apps, die nicht mehr verwendet werden?

Die meisten österreichischen App-UserInnen **löschen** Programme, die sie nicht mehr verwenden. Durchschnittlich hat jede App-UserIn bereits acht nicht mehr verwendete Apps wieder gelöscht.





Daten frei Haus

Konsumenten sind sorglos mit persönlichen Daten

- Grundsatz: „So wenig wie möglich, so viel wie nötig.“
- Bequemlichkeit siegt oft.
- Wissenschaftler warnen angesichts der rasant wachsenden Zahl von elektronischen Dienstleistungen vor allzu sorglosem Umgang mit privaten Daten. Laut einem Forschungsprojekt von sechs europäischen Institutionen zur Technikfolgenabschätzung – darunter das Institut für Technikfolgenabschätzung (ITA) der Österreichischen Akademie der Wissenschaften (ÖAW) – wird der Stellenwert der Privatsphäre sowohl durch Bürger und Unternehmen als auch durch Politiker unterschätzt. Das Projekt wird am 28. Februar im Rahmen eines Workshops mit Mitgliedern des Europäischen Parlaments, Interessenvertretern und Wissenschaftlern in Brüssel präsentiert.

Der rasante Fortschritt elektronischer Dienstleistungen birgt laut den Experten Chancen und Risiken. Internet- oder Handynutzer profitieren durch die Möglichkeiten der Technik, hinterlassen dabei aber auch Datenspuren. Die Wissenschaftler fordern, dass sich die Politik des Themas Privatsphäre annimmt.

Neue Technologien wie RFID – von Kritikern auch „Schnüffelchips“ genannt – oder Biometrie entwickeln sich sehr schnell und schaffen neue Angebote. Damit verbunden sind Gefahren für die Privatsphäre des Einzelnen. Die Anbieter sammeln, analysieren und speichern auf unbestimmte Zeit laufend verschiedenste Daten ihrer Kunden.

Unabschätzbare Folgen

Obwohl vielen Nutzern bekannt ist, wie viele persönliche Informationen sie im Umgang mit Informations- und Kommunikationstechnologien offen legen, kann von ihnen nicht erwartet werden, dass sie die langfristigen Folgen ermessen können. Aus diesem Grund

fordert Walter Peissl vom ITA eine stärkere Sensibilisierung der Anwender von elektronischen Dienstleistungen rund um das Thema Privatsphäre. In ihrem Projektbericht stellen die Forscher fest, dass der Schutz der Privatsphäre oft gegenüber Werten wie Bequemlichkeit, Sicherheit, ökonomischen Vorteilen oder sozialer Interaktion abgewogen wird. Die Experten sind überzeugt, dass viele Probleme im Zusammenhang mit Privacy vermieden werden könnten. Dazu müssten die Anliegen des Datenschutzes frühzeitig, also bereits bei der Konzeption und Entwicklung elektronischer Angebote, berücksichtigt werden. Eine obligatorische Privacy-Folgenabschätzung könnte hierzu beitragen. Beim Erheben personenbezogener Daten sollte immer der Grundsatz befolgt werden: „So wenig wie möglich, nur so viel wie nötig.“ Für Überwachungssysteme seien Aufsichtsstellen einzurichten. Weiters sollten Bürger einfachen Zugang zu den über sie gespeicherten Daten erhalten. Nicht zuletzt sollten Datenschutzbehörden mit mehr Kompetenzen und Ressourcen ausgestattet werden.

Quelle: Wiener Zeitung / www.wienerzeitung.at/nachrichten/panorama/chronik/106034_Daten-frei-Haus.html



Analysefragen



1. Vor welchem Problem warnen die in diesem Artikel zitierten Wissenschaftler?

.....

.....

2. Welche Leistungen bzw. Angebote fallen deiner Ansicht nach unter den Begriff „elektronische Dienstleistungen“?

.....

.....

3. Hast du schon einmal von „RFID“ gehört? Was könnte damit bzw. mit dem Begriff „Schnüffelchips“ gemeint sein?

.....

.....

4. Hast du schon einmal von „Biometrie“ gehört? Was könnte mit diesem Begriff gemeint sein?

.....

.....

5. In dem Artikel ist die Rede von privaten und personenbezogenen Daten. Welche Daten sind deiner Ansicht nach damit gemeint?

.....

.....

6. Im Artikel werden einige Gründe dafür angeführt, warum NutzerInnen mit ihren Daten sorglos umgehen. Welche Gründe sind das?

1.
2.
3.
4.



7. *Fallen dir noch weitere Gründe ein, die für einen sorglosen Umgang mit Daten verantwortlich sein könnten?*

.....

.....

8. *Welche Lösungsvorschläge werden im Artikel angeführt?*

.....

.....

.....

9. *Dieser Artikel stammt aus dem Jahr 2007. Denkst du, dass das darin geschilderte Problem noch aktuell ist?*

.....

.....

.....

10. *Wie schätzt du deinen Umgang mit privaten Daten ein? Wie hoch schätzt du das Risiko ein, dass deine Daten missbräuchlich verwendet werden könnten?*

.....

.....

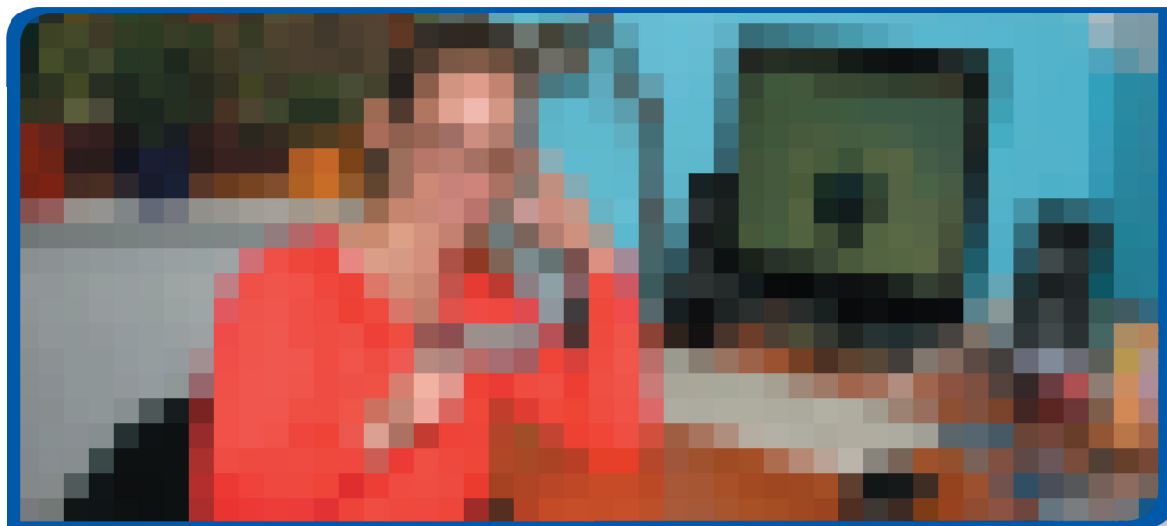
.....

11. *Welche Daten auf deinem Handy sind für dich „private“ Daten und sollten es auch bleiben?*

- ☐ SMS
- ☐ Fotos
- ☐ MMS
- ☐ Termine
- ☐ Telefonnummern
- ☐ Anruferverzeichnis



Der moderne Mensch – eine wandelnde Datenbank





Achtung – sensibel!



Alle Daten, die sich auf uns beziehen, sind persönliche Daten. Im österreichischen Datenschutzgesetz werden sie als „personenbezogene Daten“ bezeichnet. Einige der persönlichen Daten gelten als besonders sensibel.

Was denkst du – welche der angeführten Daten sind sensible Daten?

Daten	Ja	Nein
Adresse		
Allergien		
Alter		
Augenfarbe		
E-Mail-Adresse		
Entscheidung bei der letzten Nationalratswahl		
Familienstand		
Geburtsdatum		
Geburtstag		
Gewerkschaftsmitgliedschaft		
Haarfarbe		
Handynummer		
Impfpass		
IP-Adresse des Computers		
Körpergröße		
Lieblingsfarbe		
Lieblingsspeise		
Mitgliedschaft in einem Sportverein		
Mitgliedschaft in einem Verein zur Förderung der Gleichstellung von Homosexuellen		
Musikgeschmack		
Name		
Parteienmitgliedschaft		
Religionszugehörigkeit		
Schuhgröße		
Schule/Beruf		
Staatsangehörigkeit		

Achtung – sensibel!

Allergien

**Entscheidung bei der
letzten Wahl**

Familienstand

Gewerkschaftsmitgliedschaft

Impfpass

**Mitgliedschaft in einem
Verein zur Förderung der
Gleichstellung von
Homosexuellen**

Parteienmitgliedschaft

Religion

Staatsangehörigkeit



Besonders schutzwürdig?

Das österreichische Datenschutzgesetz regelt, wer welche Daten verwenden darf, welche Schritte österreichische Unternehmen setzen müssen, um die Sicherheit von Daten zu garantieren, und welche staatlichen Einrichtungen den Datenschutz kontrollieren. Außerdem gibt es einen eigenen Abschnitt zur Videoüberwachung.

Beantworte mit Hilfe des österreichischen Datenschutzgesetzes die folgenden Fragen.

1. In Artikel 1 des Datenschutzgesetzes ist das Recht auf Geheimhaltung deiner Daten festgehalten. Auf welche Daten bezieht sich die Geheimhaltung? Welche Einschränkungen werden definiert?

.....

.....

.....

Welche Rechte hast du in Bezug auf deine Daten?

.....

.....

2. Welcher Abschnitt bzw. Paragraph (§) definiert besonders schutzwürdige Daten?

.....

Wie lautet diese Definition?

.....

.....

.....

.....

3. In Artikel 2 werden Ausnahmen zur Geheimhaltungspflicht definiert. Führe den entsprechenden Abschnitt und den/die Paragraphen an!

.....

Nenne ein Beispiel für eine solche Ausnahme!

.....

.....

4. Welche Kontrollorgane gibt es in Österreich zur Wahrung des Datenschutzes?

.....

.....

Österreichisches Datenschutzgesetz

Artikel 1 (Verfassungsbestimmung) Grundrecht auf Datenschutz

§1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art.8 Abs.2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr.210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(5) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.

§2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

§3. (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.

(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

(3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden.

(4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

Artikel 2

1. Abschnitt

Allgemeines

Definitionen

§ 4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

„Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;

„sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;

„Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;

Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;

Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (Z 8);

„Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;

„Datenanwendung“: die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);

Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;

Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittels (Z 12) von Daten;

Überlassen von Daten: die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (Z 5);

Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;

„Informationsverbundsystem“: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;

„Zustimmung“: die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;

„Niederlassung“: jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.

Öffentlicher und privater Bereich

§ 5. (1) Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Bundesgesetzes zuzurechnen, wenn sie für Zwecke eines Auftraggebers des öffentlichen Bereichs (Abs. 2) durchgeführt werden.

(2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

(3) Die dem Abs. 2 nicht unterliegenden Auftraggeber gelten als Auftraggeber des privaten Bereichs im Sinne dieses Bundesgesetzes.

2. Abschnitt Verwendung von Daten

Grundsätze

§ 6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
 2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
 3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
 4. so verwendet werden, daß sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
 5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.
- (2) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.
- (3) Der Auftraggeber einer diesem Bundesgesetz unterliegenden Datenanwendung hat, wenn er nicht im Gebiet der Europäischen Union niedergelassen ist, einen in Österreich ansässigen Vertreter zu benennen, der unbeschadet der Möglichkeit eines Vorgehens gegen den Auftraggeber selbst namens des Auftraggebers verantwortlich gemacht werden kann.
- (4) Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben erachtet hat.

Zulässigkeit der Verwendung von Daten

§ 7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und
2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, daß die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und daß die Grundsätze des § 6 eingehalten werden.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

§ 8. (1) Schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder
4. überwiegende berechnete Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung zulässigerweise veröffentlichter Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.

(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat oder
7. im Katastrophenfall, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist; im letztgenannten Fall gilt § 48a Abs. 3.

(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder
2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder
3. sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Bundesgesetz gewährleistet oder
4. die Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlungen (Unterlassungen) zuständige Behörde erfolgt.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 9. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46, zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 oder im Katastrophenfall gemäß § 48a verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hierbei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

§ 10. (1) Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister die hierfür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen.

(2) Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegt, ist der Datenschutzkommission mitzuteilen, es sei denn, daß die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht. Kommt die Datenschutzkommission zur Auffassung, daß die geplante Inanspruchnahme eines Dienstleisters geeignet ist, schutzwürdige Geheimhaltungsinteressen der Betroffenen zu gefährden, so hat sie dies dem Auftraggeber unverzüglich mitzuteilen. Im übrigen gilt § 30 Abs. 6 Z 4.

Pflichten des Dienstleisters

§ 11. (1) Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber jedenfalls folgende Pflichten:

1. die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;

2. alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
3. weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, daß er dies allenfalls untersagen kann;
4. - sofern dies nach der Art der Dienstleistung in Frage kommt - im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;
5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;
6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen notwendig sind.

(2) Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der in Abs. 1 genannten Pflichten sind zum Zweck der Beweissicherung schriftlich festzuhalten.

Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

§ 12. (1) Die Übermittlung und Überlassung von Daten an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes ist keinen Beschränkungen im Sinne des § 13 unterworfen. Dies gilt nicht für den Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

(2) Keiner Genehmigung gemäß § 13 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird unter Beachtung des § 55 Z 1 durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des § 6 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

(3) Darüberhinaus ist der Datenverkehr ins Ausland dann genehmigungsfrei, wenn

1. die Daten im Inland zulässigerweise veröffentlicht wurden oder
2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden oder
3. die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder
4. Daten aus Datenanwendungen für private Zwecke (§ 45) oder für publizistische Tätigkeit (§ 48) übermittelt werden oder
5. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat oder
6. ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann oder
7. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden, oder
8. die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2 Z 6) oder Musterverordnung (§ 19 Abs. 2) ausdrücklich angeführt ist oder
9. es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt oder
10. Übermittlungen oder Überlassungen aus Datenanwendungen erfolgen, die gemäß § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

(4) Wenn eine Übermittlung oder Überlassung von Daten ins Ausland in Fällen, die von den vorstehenden Absätzen nicht erfaßt sind,

1. zur Wahrung eines wichtigen öffentlichen Interesses oder
2. zur Wahrung eines lebenswichtigen Interesses einer Person notwendig und so dringlich ist, daß die gemäß § 13 erforderliche Genehmigung der Datenschutzkommission nicht eingeholt werden kann, ohne die genannten Interessen zu gefährden, darf sie ohne Genehmigung vorgenommen werden, muß aber der Datenschutzkommission umgehend mitgeteilt werden.

(5) Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung in das Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland gemäß § 7. Bei Überlassungen ins Ausland muß darüber hinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber - oder in den Fällen des § 13 Abs. 5 an den inländischen Dienstleister - vorliegen, daß er die Dienstleisterpflichten gemäß § 11 Abs. 1 einhalten werde. Dies entfällt, wenn die Dienstleistung im Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind.

Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

§ 13. (1) Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzkommission (§§ 35 ff) einzuholen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden.

(2) Die Genehmigung ist unter Beachtung der gemäß § 55 Z 2 ergangenen Kundmachungen zu erteilen, wenn die Voraussetzungen des § 12 Abs. 5 vorliegen und wenn, ungeachtet des Fehlens eines im Empfängerstaat generell geltenden angemessenen Datenschutzniveaus,



1. für die im Genehmigungsantrag angeführte Übermittlung oder Überlassung im konkreten Einzelfall angemessener Datenschutz besteht; dies ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenverwendung eine Rolle spielen, wie insbesondere die Art der verwendeten Daten, die Zweckbestimmung sowie die Dauer der geplanten Verwendung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen, Standesregeln und Sicherheitsstandards; oder
2. der Auftraggeber glaubhaft macht, daß die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers sowie einseitige Zusagen des Antragstellers (§ 19 Abs. 2) im Genehmigungsantrag über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein. Einseitige Zusagen des Antragstellers werden für diesen mit der Registrierung durch die Datenschutzkommission verbindlich.

(3) Bei meldepflichtigen Datenanwendungen hat die Datenschutzkommission eine Ausfertigung jedes Bescheides, mit dem eine Übermittlung oder Überlassung von Daten in das Ausland genehmigt wurde, zum Registrierungsakt zu nehmen und die Erteilung der Genehmigung im Datenverarbeitungsregister (§ 16) anzumerken.

(4) Abweichend von Abs. 1 kann auch ein inländischer Dienstleister die Genehmigung beantragen, wenn er zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber mehreren Auftraggebern jeweils einen bestimmten weiteren Dienstleister im Ausland heranziehen will. Die tatsächliche Überlassung darf jeweils nur mit Zustimmung des Auftraggebers erfolgen. Der Auftraggeber hat der Datenschutzkommission mitzuteilen, aus welcher seiner meldepflichtigen Datenanwendungen die dem Dienstleister genehmigte Überlassung erfolgen soll; dies ist im Datenverarbeitungsregister anzumerken.

(5) Die Übermittlung von Daten an ausländische Vertretungsbehörden oder zwischenstaatliche Einrichtungen in Österreich gilt hinsichtlich der Pflicht zur Einholung von Genehmigungen nach Abs. 1 als Datenverkehr mit dem Ausland.

(6) Hat der Bundeskanzler trotz Fehlens eines im Empfängerstaat generell geltenden angemessenen Schutzniveaus durch Verordnung festgestellt, daß für bestimmte Kategorien des Datenverkehrs mit diesem Empfängerstaat die Voraussetzungen gemäß Abs. 2 Z 1 zutreffen, tritt an die Stelle der Verpflichtung zur Einholung einer Genehmigung die Pflicht zur Anzeige an die Datenschutzkommission. Die Datenschutzkommission hat binnen sechs Wochen ab Einlangen der Anzeige mit Bescheid den angezeigten Datenverkehr zu untersagen, wenn er keiner der in der Verordnung geregelten Kategorien zuzurechnen ist oder den Voraussetzungen gemäß § 12 Abs. 5 nicht entspricht; andernfalls ist die Übermittlung oder Überlassung der Daten in das Ausland zulässig.

3. Abschnitt Datensicherheit

Datensicherheitsmaßnahmen

§14. (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(3) Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, daß dem Betroffenen Auskunft gemäß § 26 gegeben werden kann. In der Standardverordnung (§ 17 Abs. 2 Z 6) oder in der Musterverordnung (§ 19 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten

Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, daß es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.

(5) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

(6) Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, daß sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

Datengeheimnis

§ 15. (1) Auftraggeber, Dienstleister und ihre Mitarbeiter - das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis - haben Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, daß sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeits(Dienst)verhältnisses zum Auftraggeber oder Dienstleister einhalten werden.

(3) Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen die Bestimmungen dieses Bundesgesetzes kein Nachteil erwachsen.

4. Abschnitt

Publizität der Datenanwendungen

Datenverarbeitungsregister

§ 16. (1) Die Datenschutzkommission hat ein Register der Auftraggeber mit den von ihnen betriebenen Datenanwendungen zum Zweck der Information der Betroffenen zu führen.

(2) Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, daß er Betroffener ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Auftraggebers oder anderer Personen entgegenstehen.

(3) Der Bundeskanzler hat die näheren Bestimmungen über die Führung des Registers durch Verordnung zu erlassen. Dabei ist auf die Richtigkeit und Vollständigkeit des Registers, die Übersichtlichkeit und Aussagekraft der Eintragungen und die Einfachheit der Einsichtnahme Bedacht zu nehmen.

Meldepflicht des Auftraggebers

§ 17. (1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken (Änderungsmeldung). Für manuelle Dateien besteht eine Meldepflicht nur, soweit die Inhalte zumindest einen der Tatbestände des § 18 Abs. 2 Z 1 bis 3 erfüllen.

(1a) Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte (§ 2 Z 10 des E-Government-Gesetzes, BGBl. I Nr. 10/2004) erfolgen. Nähere Bestimmungen über die Identifizierung und Authentifizierung sind in die gemäß § 16 Abs. 3 zu erlassende Verordnung aufzunehmen. Eine Meldung in Form von E-Mail oder in nicht-elektronischer Form ist für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.

(2) Nicht meldepflichtig sind Datenanwendungen, die

1. ausschließlich veröffentlichte Daten enthalten oder
2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses oder
3. nur indirekt personenbezogene Daten enthalten oder
4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) oder
5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden oder
6. einer Standardanwendung entsprechen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.



(3) Weiters sind Datenanwendungen für Zwecke

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherstellung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist.

Aufnahme der Verarbeitung

§ 18. (1) Der Vollbetrieb einer meldepflichtigen Datenanwendung darf - außer in den Fällen des Abs. 2 - unmittelbar nach Abgabe der Meldung aufgenommen werden.

(2) Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in § 48a Abs. 1 genannten Zwecke betreffen, dürfen, wenn sie

1. sensible Daten enthalten oder
2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder
3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder
4. in Form eines Informationsverbundsystems durchgeführt werden sollen, erst nach ihrer Prüfung (Vorabkontrolle) durch die Datenschutzkommission nach den näheren Bestimmungen des § 20 aufgenommen werden.

Notwendiger Inhalt der Meldung

§ 19. (1) Eine Meldung im Sinne des § 17 hat zu enthalten:

1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 3 oder eines Betreibers gemäß § 50 Abs. 1, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben, und
- 3a. die Erklärung, ob die Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 oder § 50c Abs. 1 zweiter Satz genannten Tatbestände für die Vorabkontrollpflicht erfüllt, und
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und
5. die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise - einschließlich allfälliger ausländischer Empfängerstaaten - sowie die Rechtsgrundlagen der Übermittlung und
6. - soweit eine Genehmigung der Datenschutzkommission notwendig ist - die Geschäftszahl der Genehmigung durch die Datenschutzkommission sowie
7. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

(2) Der Auftraggeber kann bei Einbringung der Meldung oder danach bis zum Abschluss des Registrierungsverfahrens zusagen, dass er sich beim Betrieb der Datenanwendung bestimmten Auflagen oder Bedingungen unterwerfen oder die Datenanwendung nur befristet betreiben wird. Eine derartige Zusage wird für den Auftraggeber mit der Registrierung durch die Datenschutzkommission rechtsverbindlich. Eine Registrierung darf nur erfolgen, wenn die zugesagte Auflage, Bedingung oder Befristung derart bestimmt ist, dass sie auch von der Datenschutzkommission nach § 21 Abs. 2 ausgesprochen werden könnte.

(3) Wenn eine größere Anzahl von Auftraggebern gleichartige Datenanwendungen vorzunehmen hat und die Voraussetzungen für die Erklärung zur Standardanwendung nicht vorliegen, kann der Bundeskanzler durch Verordnung Musteranwendungen festlegen. Meldungen über Datenanwendungen, die inhaltlich einer Musteranwendung entsprechen, müssen nur folgendes enthalten:

1. die Bezeichnung der Datenanwendung gemäß der Musterverordnung und
2. die Bezeichnung und Anschrift des Auftraggebers sowie den Nachweis seiner gesetzlichen Zuständigkeit oder seiner rechtlichen Befugnis, soweit dies erforderlich ist, und
3. die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde.

(4) Eine Meldung ist mangelhaft, wenn Angaben fehlen, offenbar unrichtig, unstimmig oder so unzureichend sind, daß Einsichtnehmer im Hinblick auf die Wahrnehmung ihrer Rechte nach diesem Bundesgesetz keine hinreichende Information darüber gewinnen können, ob durch die Datenanwendung ihre schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer gemeldeten Datenanwendung durch die gemeldeten Rechtsgrundlagen nicht gedeckt ist.

Prüfungs- und Verbesserungsverfahren

§ 20. (1) Meldungen von Datenanwendungen, die nach Angabe des Auftraggebers nicht einen der Tatbestände des § 18 Abs. 2 Z 1 bis 4 erfüllen, sind nur automationsunterstützt auf ihre Vollständigkeit und Plausibilität zu prüfen. Ist demnach die Meldung nicht fehlerhaft, so ist sie sofort zu registrieren.

(2) Wird bei der automationsunterstützten Prüfung ein Fehler der Meldung festgestellt, so ist dem Auftraggeber die Möglichkeit zur Verbesserung einzuräumen. Gleichzeitig ist er darauf hinzuweisen, dass die Meldung als nicht eingebracht gilt, wenn keine Verbesserung erfolgt oder er auf der Einbringung der unverbesserten Meldung besteht. Im letztgenannten Fall kann der Einbringer die Meldung schriftlich unter Anschluss der ausgedruckten Fehlermeldung der Datenschutzkommission übermitteln, welche die Meldung auf Mangelhaftigkeit im Sinn des § 19 Abs. 4 zu prüfen hat.

(3) Meldungen, die der Auftraggeber als vorabkontrollpflichtig bezeichnet hat oder von diesem zulässigerweise nicht im Wege der Internetanwendung (§ 17 Abs. 1a) eingebracht wurden, sind auf Mangelhaftigkeit im Sinn des § 19 Abs. 4 zu prüfen.

(4) Ergibt die Prüfung nach § 19 Abs. 4 eine Mangelhaftigkeit der Meldung, so ist dem Auftraggeber innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung unter Setzung einer angemessenen Frist aufzutragen. Im Verbesserungsauftrag ist auf die Rechtsfolgen einer Nichtbefolgung nach Abs. 5 hinzuweisen.

(5) Wird dem Verbesserungsauftrag nicht entsprochen, ist die Registrierung der Meldung durch eine schriftliche Mitteilung abzulehnen. In die Mitteilung sind aufzunehmen:

1. die Punkte, in denen der Verbesserungsauftrag nicht erfüllt wurde und
2. der Hinweis, dass innerhalb von zwei Wochen ab Zustellung bei der Datenschutzkommission ein Antrag gestellt werden kann, über die Ablehnung mit Bescheid abzusprechen.

Nach Absendung der Mitteilung erstattete Verbesserungen sind nicht zu berücksichtigen.

Registrierung

§ 21. (1) Meldungen gemäß § 19 sind in das Datenverarbeitungsregister einzutragen, wenn

1. das Prüfungsverfahren nach § 20 Abs. 1 keinen Fehler ergeben hat oder
 2. das Prüfungsverfahren nach § 20 Abs. 2 und 3 keine Mangelhaftigkeit der Meldung ergeben hat oder
 3. nach Einlangen einer auf Mangelhaftigkeit zu prüfenden Meldung bei der Datenschutzkommission zwei Monate verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 4 erteilt wurde oder
 4. der Auftraggeber die aufgetragenen Verbesserungen (§ 20 Abs. 2 und 4) vorgenommen hat.
- Die in der Meldung enthaltenen Angaben über Datensicherheitsmaßnahmen sind im Register nicht ersichtlich zu machen.

(2) Bei Datenanwendungen, die gemäß § 18 der Vorabkontrolle unterliegen, können auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen, Bedingungen oder Befristungen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit dies zur Wahrung der durch dieses Bundesgesetz geschützten Interessen der Betroffenen notwendig ist.

(3) Der Auftraggeber ist von der Durchführung und vom Inhalt der Registrierung in geeigneter Weise zu verständigen.

(4) Jedem Auftraggeber ist bei der erstmaligen Registrierung eine Registernummer zuzuteilen.

(5) Hat die automationsunterstützte Prüfung nach § 20 Abs. 1 keine Fehlerhaftigkeit der Meldung ergeben, so ist in die Registrierung ein Vermerk aufzunehmen, dass der Meldungsinhalt nur automationsunterstützt geprüft wurde.

Richtigstellung des Registers und Rechtsnachfolge

§ 22. (1) Streichungen aus dem Register und sonstige Änderungen des Registers sind auf Grund einer Änderungsmeldung des registrierten Auftraggebers oder von Amts wegen in den Fällen des Abs. 2, des § 22a Abs. 2 und des § 30 Abs. 6a vorzunehmen. Derartige Änderungen sind für die Dauer von sieben Jahren ersichtlich zu machen.

(2) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist dieser von Amts wegen aus dem Register zu streichen. Außerdem ist eine registrierte Datenanwendung zu streichen, wenn eine Befristung des Betriebes (§ 19 Abs. 2, § 21 Abs. 2) abgelaufen ist oder der Datenschutzkommission zur Kenntnis gelangt, dass die Datenanwendung dauerhaft nicht mehr betrieben wird.

(3) Berichtigungen oder Streichungen nach Abs. 2 sind ohne weiteres Ermittlungsverfahren durch Mandatsbescheid (§ 38) zu verfügen.

(4) Der Rechtsnachfolger eines registrierten Auftraggebers kann einzelne oder alle registrierten Meldungen des Rechtsvorgängers übernehmen, wenn er innerhalb von sechs Monaten nach Wirksamkeit der Rechtsnachfolge eine entsprechend glaubhaft gemachte Erklärung gegenüber der Datenschutzkommission abgibt. Dem Rechtsnachfolger kann auf Antrag auch die Registernummer des Rechtsvorgängers übertragen werden, wenn der Rechtsvorgänger jegliche Verarbeitung personenbezogener Daten in Auftraggebereigenschaft eingestellt hat.

Verfahren zur Überprüfung der Erfüllung der Meldepflicht

§ 22a. (1) Die Datenschutzkommission kann jederzeit die Erfüllung der Meldepflicht durch einen Auftraggeber prüfen. Dies gilt sowohl für die Mangelhaftigkeit einer registrierten Meldung im Sinn des § 19 Abs. 4 als auch für die rechtswidrige Unterlassung von Meldungen.

(2) Bei Vorliegen des Verdachtes der Nichterfüllung der Meldepflicht infolge Mangelhaftigkeit einer registrierten Meldung (Abs. 1) oder Unterlassung der Meldung, die über die Fälle des § 22 Abs. 2 hinausgeht, ist ein Verfahren zur Berichtigung des Datenverarbeitungsregisters durchzuführen. Das Verfahren wird durch begründete Verfahrensordnung eingeleitet, die dem meldepflichtigen Auftraggeber mit einem Auftrag zur Verbesserung (§ 20 Abs. 4) oder einer Aufforderung zur Nachmeldung (§ 17 Abs. 1) innerhalb gesetzter Frist zuzustellen ist.



(3) Wird einem im Verfahren nach Abs. 2 erteilten Verbesserungsauftrag nicht entsprochen, so ist die Streichung der Meldung mit Bescheid der Datenschutzkommission zu verfügen. Die Streichung kann sich, wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Herstellung des rechtmäßigen Zustandes ausreichend ist, auch nur auf Teile der Meldung beschränken.

(4) Wird einer im Verfahren nach Abs. 2 erteilten Aufforderung zur Nachmeldung nicht entsprochen und die Unterlassung einer Meldung entgegen § 17 Abs. 1 erwiesen, so ist mit Bescheid der Datenschutzkommission der weitere Betrieb der Datenanwendung, soweit er vom Registerstand abweicht, zu untersagen und gleichzeitig Anzeige nach § 52 Abs. 2 Z 1 an die zuständige Behörde zu erstatten.

(5) Ergibt das Verfahren nach Abs. 2 alleine die Unangemessenheit oder die Nichteinhaltung von nach § 19 Abs. 1 Z 7 erklärten Datensicherheitsmaßnahmen, so ist dies mit Bescheid festzustellen und gleichzeitig eine angemessene Frist zur Herstellung ausreichender Datensicherheit zu setzen. Der Auftraggeber hat innerhalb dieser Frist der Datenschutzkommission die getroffenen Maßnahmen mitzuteilen. Sind diese nicht ausreichend, so ist die Streichung der Datenanwendung zu verfügen.

(6) Die Einleitung und der Stand eines Berichtigungsverfahrens nach Abs. 2 ist bei registrierten Meldungen im Datenverarbeitungsregister bis zur Einstellung oder bis zur Herstellung eines rechtmäßigen Zustandes durch Maßnahmen nach den Abs. 3 bis 6 geeignet anzumerken.

Pflicht zur Offenlegung nicht-meldepflichtiger Datenanwendungen

§ 23. (1) Auftraggeber einer Standardanwendung haben jedermann auf Anfrage mitzuteilen, welche Standardanwendungen sie tatsächlich vornehmen.

(2) Nicht-meldepflichtige Datenanwendungen sind der Datenschutzkommission bei Ausübung ihrer Kontrollaufgaben gemäß § 30 offenzulegen.

Informationspflicht des Auftraggebers

§ 24. (1) Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und
2. über Namen und Adresse des Auftraggebers, zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.

(2) Über Abs. 1 hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist; dies gilt insbesondere dann, wenn

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder
2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder
3. Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne daß dies gesetzlich vorgesehen ist.

(2a) Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert.

(3) Werden Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt, darf die Information gemäß Abs. 1 entfallen, wenn

1. die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist oder
2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder
3. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 46 oder Adreßdaten im Rahmen des § 47 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Der Bundeskanzler kann durch Verordnung weitere Fälle festlegen, in welchen die Pflicht zur Information entfällt.

(4) Keine Informationspflicht nach Abs. 1 besteht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 und 3 nicht meldepflichtig sind.

Pflicht zur Offenlegung der Identität des Auftraggebers

§ 25. (1) Bei Übermittlungen und bei Mitteilungen an Betroffene hat der Auftraggeber seine Identität in geeigneter Weise offenzulegen, sodaß den Betroffenen die Verfolgung ihrer Rechte möglich ist. Bei meldepflichtigen Datenanwendungen ist in Mitteilungen an Betroffene die Registernummer des Auftraggebers anzuführen.

(2) Werden Daten aus einer Datenanwendung für Zwecke einer vom Auftraggeber verschiedenen Person verwendet, ohne daß diese ihrerseits ein Verfügungsrecht über die verwendeten Daten und damit die Eigenschaft eines Auftraggebers in Bezug auf die Daten erlangt, dann ist bei Mitteilungen an den Betroffenen neben der Identität der Person, für deren Zwecke die Daten verwendet werden, auch die Identität des Auftraggebers anzugeben, aus dessen Datenanwendung die Daten stammen. Handelt es sich hierbei um eine meldepflichtige Datenanwendung, ist die Registernummer des Auftraggebers beizufügen. Diese Pflicht trifft sowohl den Auftraggeber als auch denjenigen, in dessen Namen die Mitteilung an den Betroffenen erfolgt.

5. Abschnitt Die Rechte des Betroffenen

Auskunftsrecht

§ 26. (1) Ein Auftraggeber hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist, Auskunft über die zu dieser Person oder Personengemeinschaft verarbeiteten Daten zu geben. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hierfür in allgemein verständlicher Form anzuführen. Auf Verlangen eines Betroffenen sind auch Namen und Adressen von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft). Mit Zustimmung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des Auskunftswerbers aus besonderen Gründen notwendig ist oder soweit überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hierbei aus der Notwendigkeit

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.

(3) Der Auskunftswerber hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Auskunftswerber am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen: Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, daß keine der Auskunftspflicht unterliegenden Daten über den Auskunftswerber verwendet werden. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Auskunftswerber im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten. Diese Frist gilt nicht, wenn einem Löschantrag des Auskunftswerbers nach § 27 Abs. 1 Z 2 oder § 28 zu entsprechen ist.

(8) In dem Umfang, in dem eine Datenanwendung für eine Person oder Personengemeinschaft hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, hat diese das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen. Für das Verfahren der Einsichtnahme (einschließlich deren Verweigerung) gelten die näheren Regelungen des Gesetzes, das das Einsichtsrecht vorsieht. In Abs. 1 genannte Bestandteile einer Auskunft, die vom Einsichtsrecht nicht umfasst sind, können dennoch nach diesem Bundesgesetz geltend gemacht werden.

(9) Für Auskünfte aus dem Strafregister gelten die besonderen Bestimmungen des Strafregistergesetzes 1968 über Strafregisterbescheinigungen.

(10) Ergibt sich eine Auftraggeberstellung auf Grund von Rechtsvorschriften, obwohl die Datenverarbeitung für Zwecke der Auftragserfüllung für einen Dritten erfolgt (§ 4 Abs. 1 Z 4 letzter Satz), kann der Auskunftswerber sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Auskunftswerber, soweit ihm dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des tatsächlichen Auftraggebers mitzuteilen, damit der Auskunftswerber sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann. Wird ein Auskunftsbegehren an einen Dienstleister gerichtet und lässt dieses erkennen, dass der Auskunftswerber ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Dienstleister das Auskunftsbegehren unverzüglich an den Auftraggeber weiterzuleiten und dem Auskunftswerber mitzuteilen, dass in seinem Auftrag keine Daten verwendet werden. D



Der Auftraggeber hat innerhalb von acht Wochen ab Einlangen des Auskunftsbegehens beim Dienstleister dem Auskunftswerber Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, von einer Auskunftserteilung abzusehen. Wird jedoch in weiterer Folge das Ersuchen direkt an den Auftraggeber gestellt, so hat dieser nach Abs. 5 vorzugehen. Für Betreiber von Informationsverbundsystemen gilt jedoch ausschließlich § 50 Abs. 1.

Recht auf Richtigstellung oder Löschung

§ 27. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder
2. auf begründeten Antrag des Betroffenen.

Der Pflicht zur Richtigstellung nach Z 1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§ 46 und 47.

(2) Der Beweis der Richtigkeit der Daten obliegt - sofern gesetzlich nicht ausdrücklich anderes angeordnet ist - dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

(3) Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zuläßt. Die erforderlichen Richtigstellungen sind diesfalls durch entsprechende zusätzliche Anmerkungen zu bewirken.

(4) Innerhalb von acht Wochen nach Einlangen eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in § 26 Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Geheimhaltung erfordern, mit einem Richtigstellungs- oder Löschantrag folgendermaßen zu verfahren: Die Richtigstellung oder Löschung ist vorzunehmen, wenn das Begehren des Betroffenen nach Auffassung des Auftraggebers berechtigt ist. Die gemäß Abs. 4 erforderliche Mitteilung an den Betroffenen hat in allen Fällen dahingehend zu lauten, daß die Überprüfung der Datenbestände des Auftraggebers im Hinblick auf das Richtigstellungs- oder Löschantragsbegehren durchgeführt wurde. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtenden Daten mit einer berichtenden Anmerkung zu versehen.

(7) Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet, und läßt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzkommission gelöscht werden.

(8) Wurden im Sinne des Abs. 1 richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Auftraggeber die Empfänger dieser Daten hiervon in geeigneter Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere im Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.

(9) Die Regelungen der Abs. 1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für öffentliche Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für

1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder
2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschanträge von Betroffenen durch Bundesgesetz nicht anderes bestimmt ist.

Widerspruchsrecht

§ 28. (1) Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen.

(2) Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datenanwendung kann der Betroffene jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben. Die Daten sind binnen acht Wochen zu löschen.

(3) § 27 Abs. 4 bis 6 gelten auch in den Fällen der Abs. 1 und 2.

Die Rechte des Betroffenen bei der Verwendung nur indirekt personenbezogener Daten

§ 29. Die durch die §§ 26 bis 28 gewährten Rechte können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.

6. Abschnitt Rechtsschutz

Kontrollbefugnisse der Datenschutzkommission

§ 30. (1) Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzkommission wenden.

(2) Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hierbei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.

(2a) Sofern sich eine zulässige Eingabe nach Abs. 1 oder ein begründeter Verdacht nach Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzkommission die Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorgehen.

(3) Datenanwendungen, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dies gilt auch für jene Bereiche der Vollziehung, in welchen ein Auftraggeber des öffentlichen Bereichs die grundsätzliche Anwendbarkeit der §§ 26 Abs. 5 und 27 Abs. 5 in Anspruch nimmt.

(4) Zum Zweck der Einschau ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen. Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglicher Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Dazu zählt auch die Verwendung für Zwecke der gerichtlichen Rechtsverfolgung durch den Einschreiter oder die Datenschutzkommission nach § 32. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes, einer strafbaren Handlung nach den §§ 118a, 119, 119a, 126a bis 126c, 148a oder § 278a des Strafgesetzbuches, BGBl. Nr. 60/1974, oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozessordnung, BGBl. Nr. 631/1975, zu entsprechen ist.

(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission, sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach Abs. 6a zu treffen sind, Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere

1. Strafanzeige nach §§ 51 oder 52 erstatten, oder
2. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder
3. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.

(6a) Liegt durch den Betrieb einer Datenanwendung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so kann die Datenschutzkommission die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51, untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Wird einer Untersagung nicht sogleich Folge geleistet, ist Strafanzeige nach § 52 Abs. 1 Z 3 zu erstatten. Nach Rechtskraft einer Untersagung nach diesem Absatz ist ein Berichtigungsverfahren nach § 22a Abs. 2 formlos einzustellen. Die Datenanwendung ist im Umfang der Untersagung aus dem Register zu streichen.

(7) Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde.

Beschwerde an die Datenschutzkommission

§ 31. (1) Die Datenschutzkommission erkennt über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Auskunft nach § 26 oder nach § 50 Abs. 1 dritter Satz oder in ihrem Recht auf Darlegung einer automatisierten Einzelentscheidung nach § 49 Abs. 3 verletzt zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Die Datenschutzkommission erkennt weiters über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Geheimhaltung (§ 1 Abs. 1) oder in ihrem Recht auf Richtigstellung oder auf Löschung (§§ 27 und 28) verletzt zu sein, sofern der Anspruch nicht nach § 32 Abs. 1 vor einem Gericht geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet.

(3) Die Beschwerde hat zu enthalten:

1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugeordnet wird (Beschwerdegegner),
3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,
4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

(4) Einer Beschwerde nach Abs. 1 sind außerdem das zu Grunde liegende Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) und eine allfällige Antwort des Beschwerdegegners anzuschließen. Einer Beschwerde nach Abs. 2 sind außerdem der zu Grunde liegende Antrag auf Richtigstellung oder Löschung und eine allfällige Antwort des Beschwerdegegners anzuschließen.

(5) Die der Datenschutzkommission durch § 30 Abs. 2 bis 4 eingeräumten Kontrollbefugnisse kommen ihr auch in Beschwerdeverfahren nach Abs. 1 und 2 gegenüber dem Beschwerdegegner zu. Ebenso besteht auch hinsichtlich dieser Verfahren die Verschwiegenheitspflicht nach § 30 Abs. 5.

(6) Im Fall der Einbringung einer zulässigen Beschwerde nach Abs. 1 oder 2 ist ein auf Grund einer Eingabe nach § 30 Abs. 1 über denselben Gegenstand eingeleitetes Kontrollverfahren durch eine entsprechende Information (§ 30 Abs. 7) zu beenden. Die Datenschutzkommission kann aber dennoch auch während der Anhängigkeit des Beschwerdeverfahrens von Amts wegen nach § 30 Abs. 2 vorgehen, wenn ein begründeter Verdacht einer über den Beschwerdefall hinausgehenden Verletzung datenschutzrechtlicher Verpflichtungen besteht. § 30 Abs. 3 bleibt unberührt.

(7) Soweit sich eine Beschwerde nach Abs. 1 oder 2 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte Verletzung im Recht auf Auskunft (Abs. 1) einem Auftraggeber des privaten Bereichs zuzurechnen, so ist diesem auf Antrag zusätzlich die – allenfalls erneute – Reaktion auf das Auskunftsbegehren nach § 26 Abs. 4, 5 oder 10 in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen.

(8) Ein Beschwerdegegner, gegen den wegen Verletzung in Rechten nach den §§ 26 bis 28 Beschwerde erhoben wurde, kann bis zum Abschluss des Verfahrens vor der Datenschutzkommission durch Reaktionen gegenüber dem Beschwerdeführer gemäß § 26 Abs. 4 oder § 27 Abs. 4 die behauptete Rechtsverletzung nachträglich beseitigen. Erscheint der Datenschutzkommission durch derartige Reaktionen des Beschwerdegegners die Beschwerde als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzkommission das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 13 Abs. 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen. Auch diesfalls ist das ursprüngliche Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen.

Begleitende Maßnahmen im Beschwerdeverfahren

§ 31a. (1) Sofern sich eine zulässige Beschwerde nach § 31 Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzkommission die Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorgehen.

(2) Macht der Beschwerdeführer im Rahmen einer Beschwerde nach § 31 Abs. 2 eine wesentliche Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen durch die Verwendung seiner Daten glaubhaft, so kann die Datenschutzkommission nach § 30 Abs. 6a vorgehen.

(3) Ist in einem Verfahren nach § 31 Abs. 2 die Richtigkeit von Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen. Erforderlichenfalls hat dies die Datenschutzkommission auf Antrag des Beschwerdeführers mit Mandatsbescheid anzuordnen.

(4) Berufte sich ein Auftraggeber des öffentlichen Bereichs bei einer Beschwerde wegen Verletzung des Auskunfts-, Richtigstellungs- oder Löschungsrechts gegenüber der Datenschutzkommission auf die §§ 26 Abs. 5 oder 27 Abs. 5, so hat diese nach Überprüfung der Notwendigkeit der Geheimhaltung die geschützten öffentlichen Interessen in ihrem Verfahren zu wahren. Kommt sie zur Auffassung, dass die Geheimhaltung von verarbeiteten Daten gegenüber dem Betroffenen nicht gerechtfertigt war, ist die Offenlegung der Daten mit Bescheid aufzutragen. Gegen diese Entscheidung der Datenschutzkommission kann die belangte Behörde Beschwerde an den Verwaltungsgerichtshof erheben. Wurde keine derartige Beschwerde eingebracht und wird dem Bescheid der Datenschutzkommission binnen acht Wochen nicht entsprochen, so hat die Datenschutzkommission die Offenlegung der Daten gegenüber dem Betroffenen selbst vorzunehmen und ihm die verlangte Auskunft zu erteilen oder ihm mitzuteilen, welche Daten bereits berichtet oder gelöscht wurden. Die ersten beiden Sätze gelten in Verfahren nach § 30 sinngemäß.



Anrufung der Gerichte

§ 32. (1) Ansprüche wegen Verletzung der Rechte einer Person oder Personengemeinschaft auf Geheimhaltung, auf Richtigstellung oder auf Löschung gegen natürliche Personen, Personengemeinschaften oder Rechtsträger, die in Formen des Privatrechts eingerichtet sind, sind, soweit diese Rechtsträger bei der behaupteten Verletzung nicht in Vollziehung der Gesetze tätig geworden sind, auf dem Zivilrechtsweg geltend zu machen.

(2) Sind Daten entgegen den Bestimmungen dieses Bundesgesetzes verwendet worden, so hat der Betroffene Anspruch auf Unterlassung und Beseitigung des diesem Bundesgesetz widerstreitenden Zustandes.

(3) Zur Sicherung der auf dieses Bundesgesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die in § 381 EO bezeichneten Voraussetzungen nicht zutreffen. Dies gilt auch für Verfügungen über die Verpflichtung zur Anbringung eines Bestreitungsvermerks.

(4) Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.

(5) Die Datenschutzkommission hat in Fällen, in welchen der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, gegen diesen eine Feststellungsklage (§ 228 ZPO) bei dem gemäß Abs. 4 zweiter Satz zuständigen Gericht zu erheben.

(6) Die Datenschutzkommission hat, wenn ein Einschreiter (§ 30 Abs. 1) es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von natürlichen Personen geboten ist, einem Rechtsstreit auf Seiten des Einschreiters als Nebenintervenient (§§ 17 ff ZPO) beizutreten.

(7) Anlässlich einer zulässigen Klage nach Abs. 1, die sich auf eine nach Ansicht des Gerichts meldepflichtige Datenanwendung bezieht, kann das Gericht die Datenschutzkommission um Überprüfung nach den §§ 22 und 22a ersuchen. Die Datenschutzkommission hat das Gericht vom Ergebnis der Überprüfung zu verständigen. Dieses ist sodann vom Gericht auch den Parteien bekannt zu geben, sofern das Verfahren noch nicht rechtskräftig beendet ist.

Schadenersatz

§ 33. (1) Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Werden durch die öffentlich zugängliche Verwendung der in § 18 Abs. 2 Z 1 bis 3 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs. 1 des Mediengesetzes, BGBl. Nr. 314/1981, gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen.

(2) Der Auftraggeber und der Dienstleister haften auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

(3) Der Auftraggeber kann sich von seiner Haftung befreien, wenn er nachweist, daß der Umstand, durch den der Schaden eingetreten ist, ihm und seinen Leuten (Abs. 2) nicht zur Last gelegt werden kann. Dasselbe gilt für die Haftungsbefreiung des Dienstleisters. Für den Fall eines Mitverschuldens des Geschädigten oder einer Person, deren Verhalten er zu vertreten hat, gilt § 1304 ABGB.

(4) Die Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 32 Abs. 4.

Gemeinsame Bestimmungen

§ 34. (1) Der Anspruch auf Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32 erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist dem Einschreiter im Falle einer verspäteten Eingabe gemäß § 30 mitzuteilen; verspätete Beschwerden nach § 31 und Klagen nach § 32 sind zurückzuweisen.

(2) Eingaben nach § 30, Beschwerden nach § 31, Klagen nach § 32 sowie Schadenersatzansprüche nach § 33 können nicht nur auf die Verletzung der Vorschriften dieses Bundesgesetzes, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaates der Europäischen Union gegründet werden, soweit solche Vorschriften gemäß § 3 im Inland anzuwenden sind.

(3) Ist ein von der Datenschutzkommission zu prüfender Sachverhalt gemäß § 3 nach der Rechtsordnung eines anderen Vertragsstaates des Europäischen Wirtschaftsraumes zu beurteilen, so kann die Datenschutzkommission die zuständige ausländische Datenschutzkontrollstelle um Unterstützung ersuchen.

(4) Die Datenschutzkommission hat den Unabhängigen Datenschutzkontrollstellen der anderen Vertragsstaaten des Europäischen Wirtschaftsraumes über Ersuchen Amtshilfe zu leisten.

7. Abschnitt Kontrollorgane

Datenschutzkommission und Datenschutzrat

§ 35. (1) Zur Wahrung des Datenschutzes sind nach den näheren Bestimmungen dieses Bundesgesetzes - unbeschadet der Zuständigkeit des Bundeskanzlers und der ordentlichen Gerichte - die Datenschutzkommission und der Datenschutzrat berufen.

(2) (Verfassungsbestimmung) Die Datenschutzkommission übt ihre Befugnisse auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung aus.

Zusammensetzung der Datenschutzkommission

§ 36. (1) Die Datenschutzkommission besteht aus sechs Mitgliedern, die auf Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt werden. Wiederbestellungen sind zulässig. Die Mitglieder müssen rechtskundig sein. Ein Mitglied muß dem Richterstand angehören.

(2) Die Vorbereitung des Vorschlages der Bundesregierung für die Bestellung der Mitglieder der Datenschutzkommission obliegt dem Bundeskanzler. Er hat dabei Bedacht zu nehmen auf:

1. einen Dreivorschlag des Präsidenten des Obersten Gerichtshofs für das richterliche Mitglied,
2. einen Vorschlag der Länder für zwei Mitglieder,
3. einen Dreivorschlag der Bundeskammer für Arbeiter und Angestellte für ein Mitglied,
4. einen Dreivorschlag der Wirtschaftskammer Österreich für ein Mitglied.

Alle vorgeschlagenen Personen sollen Erfahrung auf dem Gebiet des Datenschutzes besitzen.

(3) Ein Mitglied ist aus dem Kreise der rechtskundigen Bundesbediensteten vorzuschlagen.

(3a) Die Mitglieder der Datenschutzkommission üben diese Funktion neben ihnen sonst obliegenden beruflichen Tätigkeiten aus.

(4) Für jedes Mitglied ist ein Ersatzmitglied zu bestellen. Das Ersatzmitglied tritt bei Verhinderung des Mitglieds an dessen Stelle. Die Funktionsperiode des Ersatzmitglieds endet mit der Funktionsperiode des Mitglieds; für den Fall der vorzeitigen Beendigung der Funktionsperiode des Mitglieds gilt Abs. 8.

(5) Der Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;
2. Personen, die zum Nationalrat nicht wählbar sind.

(6) Hat ein Mitglied der Datenschutzkommission Einladungen zu drei aufeinanderfolgenden Sitzungen ohne genügende Entschuldigung keine Folge geleistet oder tritt bei einem Mitglied ein Ausschließungsgrund des Abs. 5 nachträglich ein, so hat dies nach seiner Anhörung die Datenschutzkommission festzustellen. Diese Feststellung hat den Verlust der Mitgliedschaft zur Folge. Im übrigen kann ein Mitglied der Datenschutzkommission nur aus einem schwerwiegenden Grund durch Beschluß der Datenschutzkommission, dem mindestens drei ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden. Die Mitgliedschaft endet auch, wenn das Mitglied seine Funktion durch schriftliche Erklärung an den Bundeskanzler zurücklegt. Die Mitgliedschaft des richterlichen Mitglieds sowie des Mitglieds aus dem Kreis der rechtskundigen Bundesbediensteten endet auch, wenn diese aus ihren Dienstverhältnissen zum Bund ausscheiden, in den Ruhestand übertreten oder in den Ruhestand versetzt werden. Bei Richtern steht dem Ausscheiden eine Dienstzuteilung nach § 78 des Richter- und Staatsanwaltschaftsdienstgesetzes, BGBl. Nr. 305/1961, gleich. Die Mitgliedschaft der übrigen Mitglieder endet am 31. Dezember des Jahres, in dem sie das 65. Lebensjahr vollenden.

(7) Auf die Ersatzmitglieder sind die Abs. 2, 3, 5 und 6 wie auf Mitglieder anzuwenden.

(8) Scheidet ein Mitglied wegen Todes, freiwillig oder gemäß Abs. 6 vorzeitig aus, so wird das betreffende Ersatzmitglied (Abs. 4) Mitglied der Datenschutzkommission bis zum Ablauf der Funktionsperiode des ausgeschiedenen Mitglieds. Unter Anwendung der Abs. 2 und 3 ist für diese Zeit ein neues Ersatzmitglied zu bestellen. Scheidet ein Ersatzmitglied vorzeitig aus, ist unverzüglich ein neues Ersatzmitglied zu bestellen.

(9) Die Mitglieder und Ersatzmitglieder der Datenschutzkommission haben für die Anreise zu den Sitzungen der Datenschutzkommission sowie für in Ausübung ihrer Funktion erforderliche sonstige Dienstreisen Anspruch auf Ersatz der Reisekosten (Gebühreinstufe 3) durch den Bundeskanzler nach Maßgabe der für Bundesbedienstete geltenden Rechtsvorschriften. Sie haben ferner Anspruch auf eine der Zeit und dem Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist.

Weisungsfreiheit der Datenschutzkommission

§ 37. (1) Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden.

(2) Die in der Geschäftsstelle der Datenschutzkommission tätigen Bediensteten unterstehen fachlich nur den Weisungen des Vorsitzenden oder des geschäftsführenden Mitglieds der Datenschutzkommission.

Organisation und Geschäftsführung der Datenschutzkommission

§ 38. (1) (Verfassungsbestimmung) Die Datenschutzkommission hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist (geschäftsführendes Mitglied). Diese Betrauung umfaßt

auch die Erlassung von verfahrensrechtlichen Bescheiden und von Mandatsbescheiden im Registrierungsverfahren gemäß § 20 Abs. 2 oder § 22 Abs. 3. Inwieweit einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied ermächtigt werden, bestimmt die Geschäftsordnung.

(2) Für die Unterstützung in der Geschäftsführung der Datenschutzkommission hat der Bundeskanzler eine Geschäftsstelle einzurichten und die notwendige Sach- und Personalausstattung bereitzustellen. Er hat das Recht, sich jederzeit über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten.

(3) Die Datenschutzkommission ist vor Erlassung von Verordnungen anzuhören, die auf der Grundlage dieses Bundesgesetzes ergehen oder sonst wesentliche Fragen des Datenschutzes unmittelbar betreffen.

(4) Die Datenschutzkommission hat spätestens alle zwei Jahre einen Bericht über ihre Tätigkeit zu erstellen und in geeigneter Weise zu veröffentlichen. Der Bericht ist dem Bundeskanzler zur Kenntnis zu übermitteln.

Beschlüsse der Datenschutzkommission

§ 39. (1) Die Datenschutzkommission ist bei Anwesenheit aller sechs Mitglieder beschlußfähig. Für den Fall der Verhinderung eines Mitglieds gilt § 36 Abs. 4.

(2) Das richterliche Mitglied führt den Vorsitz.

(3) Für einen gültigen Beschluß der Datenschutzkommission ist die Zustimmung der Mehrheit der abgegebenen Stimmen notwendig. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig.

(4) Entscheidungen der Datenschutzkommission von grundsätzlicher Bedeutung für die Allgemeinheit sind von der Datenschutzkommission unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.

(5) Beschlüsse der Datenschutzkommission werden vom Vorsitzenden ausgefertigt.

Wirkung von Bescheiden der Datenschutzkommission und des geschäftsführenden Mitglieds

§ 40. (1) Gegen Bescheide, die das geschäftsführende Mitglied der Datenschutzkommission gemäß § 22 Abs. 3, § 30 Abs. 6a oder § 31a Abs. 3 in Verbindung mit § 38 Abs. 1 erlassen hat, ist die Vorstellung an die Datenschutzkommission gemäß § 57 Abs. 2 AVG zulässig. Eine Vorstellung gegen einen gemäß § 22 Abs. 3 ergangenen Bescheid hat aufschiebende Wirkung.

(2) Gegen Bescheide der Datenschutzkommission ist kein Rechtsmittel zulässig. Sie unterliegen nicht der Aufhebung oder Abänderung im Verwaltungsweg. Auftraggeber des öffentlichen Bereichs haben in Verfahren vor der Datenschutzkommission stets Parteistellung. Die Anrufung des Verwaltungsgerichtshofes durch die Parteien des Verfahrens ist zulässig. Dies gilt jedoch nicht für Auftraggeber des öffentlichen Bereichs als Beschwerdegegner im Verfahren nach § 31, es sei denn es ist durch besondere gesetzliche Regelung die Möglichkeit einer Amtsbeschwerde (Art. 131 Abs. 2 B-VG) vorgesehen.

(3) Bescheide, mit welchen gemäß § 13 Übermittlungen oder Überlassungen von Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen und tatsächlichen Voraussetzungen für die Erteilung der Genehmigung, insbesondere auch infolge einer gemäß § 55 ergangenen Kundmachung des Bundeskanzlers, nicht mehr bestehen.

(4) Wenn die Datenschutzkommission eine Verletzung von Bestimmungen dieses Bundesgesetzes durch einen Auftraggeber des öffentlichen Bereichs festgestellt hat, so hat dieser mit den ihm zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung der Datenschutzkommission entsprechenden Zustand herzustellen.

Einrichtung und Aufgaben des Datenschutzrates

§ 41. (1) Beim Bundeskanzleramt ist ein Datenschutzrat eingerichtet.

(2) Der Datenschutzrat berät die Bundesregierung und die Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe

1. kann der Datenschutzrat Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen;
2. ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind;
3. haben Auftraggeber des öffentlichen Bereichs ihre Vorhaben dem Datenschutzrat zur Stellungnahme zuzuleiten, soweit diese datenschutzrechtlich von Bedeutung sind;
4. hat der Datenschutzrat das Recht, von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;
- 4a. hat der Datenschutzrat das Recht, von der Datenschutzkommission Auskünfte und Berichte sowie Einsicht in Unterlagen zu verlangen;
5. kann der Datenschutzrat Auftraggeber des privaten Bereichs oder auch ihre gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung auffordern, die aus datenschutzrechtlicher Sicht Anlaß zu Bedenken, zumindest aber Anlaß zur Beobachtung geben;
6. kann der Datenschutzrat seine Beobachtungen, Bedenken und allfälligen Anregungen zur Verbesserung des Datenschutzes in Österreich der Bundesregierung und den Landesregierungen mitteilen, sowie über Vermittlung dieser Organe den gesetzgebenden Körperschaften zur Kenntnis bringen.

(3) Abs. 2 Z 3 und 4 gilt nicht, soweit innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betroffen sind.

Zusammensetzung des Datenschutzrates

§ 42. (1) Dem Datenschutzrat gehören an:

1. Vertreter der politischen Parteien: Von der im Hauptausschuss des Nationalrates am stärksten vertretenen Partei sind vier Vertreter, von der am zweitstärksten vertretenen Partei sind drei Vertreter und von jeder anderen im Hauptausschuss des Nationalrates vertretenen Partei ist ein Vertreter in den Datenschutzrat zu entsenden, wobei es allein auf die Stärke im Zeitpunkt der Entsendung ankommt. Bei Mandatsgleichheit zweier Parteien im Hauptausschuss ist die Stimmenstärke bei der letzten Wahl zum Nationalrat ausschlaggebend;
2. je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;
3. zwei Vertreter der Länder;
4. je ein Vertreter des Gemeindebundes und des Städtebundes;
5. ein vom Bundeskanzler zu ernennender Vertreter des Bundes.

(2) Die in Abs. 1 Z 3, 4 und 5 genannten Vertreter sollen berufliche Erfahrung auf dem Gebiet der Informatik und des Datenschutzes haben.

(3) Für jedes Mitglied ist ein Ersatzmitglied namhaft zu machen.

(4) Dem Datenschutzrat können Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre und weitere Personen, die zum Nationalrat nicht wählbar sind, nicht angehören.

(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis sie dem Bundeskanzler schriftlich ihr Ausscheiden mitteilen oder, mangels einer solchen Mitteilung, von der entsendenden Stelle (Abs. 1) dem Bundeskanzler ein anderer Vertreter namhaft gemacht wird. Mitglieder nach Abs. 1 Z 1 scheiden außerdem aus, sobald der Hauptausschuss nach den §§ 29 und 30 des Geschäftsordnungsgesetzes 1975, BGBl. Nr. 410, neu gewählt wurde, und sie nicht neuerlich entsendet werden.

(6) Die Tätigkeit der Mitglieder des Datenschutzrates ist ehrenamtlich. Mitglieder des Datenschutzrates, die außerhalb von Wien wohnen, haben im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) nach Maßgabe der für Bundesbeamte geltenden Rechtsvorschriften.

Vorsitz und Geschäftsführung des Datenschutzrates

§ 43. (1) Der Datenschutzrat gibt sich mit Beschluß eine Geschäftsordnung.

(2) Der Datenschutzrat hat aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu wählen. Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden dauert - unbeschadet des § 42 Abs. 5 - fünf Jahre. Wiederbestellungen sind zulässig.

(3) Die Geschäftsführung des Datenschutzrates obliegt dem Bundeskanzleramt. Der Bundeskanzler hat das hierfür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind die Bediensteten des Bundeskanzleramtes fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.

Sitzungen und Beschlußfassung des Datenschutzrates

§ 44. (1) Die Sitzungen des Datenschutzrates werden vom Vorsitzenden nach Bedarf einberufen. Begehrt ein Mitglied die Einberufung einer Sitzung, so hat der Vorsitzende die Sitzung so einzuberufen, daß sie binnen vier Wochen stattfinden kann.

(2) Zu den Sitzungen kann der Vorsitzende nach Bedarf Sachverständige zuziehen.

(3) Für Beratungen und Beschlußfassungen im Datenschutzrat ist die Anwesenheit von mehr als der Hälfte seiner Mitglieder erforderlich. Zur Beschlußfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Die Beifügung von Minderheitenvoten ist zulässig.

(4) Der Datenschutzrat kann aus seiner Mitte ständige oder nichtständige Arbeitsausschüsse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten übertragen kann. Er ist auch berechtigt, die Geschäftsführung, Vorbereitung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatte) zu übertragen.

(5) Jedes Mitglied des Datenschutzrates ist verpflichtet, an den Sitzungen - außer im Fall der gerechtfertigten Verhinderung - teilzunehmen. Ist ein Mitglied an der Teilnahme verhindert, hat es hievon unverzüglich das Ersatzmitglied zu verständigen.

(6) Mitglieder der Datenschutzkommission, die dem Datenschutzrat nicht angehören, sind berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse teilzunehmen. Ein Stimmrecht steht ihnen nicht zu.

(7) Die Beratungen in der Sitzung des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, vertraulich.

(8) Die Mitglieder des Datenschutzrates, die anwesenden Mitglieder der Datenschutzkommission und die zur Sitzung gemäß Abs. 2 zugezogenen Sachverständigen sind zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet, sofern die Geheimhaltung im öffentlichen Interesse oder im Interesse einer Partei geboten ist.

8. Abschnitt

Besondere Verwendungszwecke von Daten

Private Zwecke

§ 45. (1) Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten verarbeiten, wenn sie ihnen

vom Betroffenen selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise, insbesondere in Übereinstimmung mit § 7 Abs. 2, zugekommen sind.

(2) Daten, die eine natürliche Person für ausschließlich persönliche oder familiäre Tätigkeiten verarbeitet, dürfen, soweit gesetzlich nicht ausdrücklich anderes vorgesehen ist, für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.

Wissenschaftliche Forschung und Statistik

§ 46. (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die

1. öffentlich zugänglich sind oder
2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für ihn nur indirekt personenbezogen sind.

Andere Daten dürfen nur unter den Voraussetzungen des Abs. 2 Z 1 bis 3 verwendet werden.

(2) Bei Datenanwendungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs. 1 fallen, dürfen Daten nur

1. gemäß besonderen gesetzlichen Vorschriften oder
2. mit Zustimmung des Betroffenen oder
3. mit Genehmigung der Datenschutzkommission gemäß Abs. 3 verwendet werden.

(3) Eine Genehmigung der Datenschutzkommission für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik ist auf Antrag des Auftraggebers der Untersuchung zu erteilen, wenn

1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und
 2. ein öffentliches Interesse an der beantragten Verwendung besteht und
 3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird.
- Sollen sensible Daten ermittelt werden, muß ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muß gewährleistet sein, daß die Daten beim Auftraggeber der Untersuchung nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

(3a) Einem Antrag nach Abs. 3 ist jedenfalls eine vom Verfügungsbefugten über die Datenbestände, aus denen die Daten ermittelt werden sollen, oder einem sonst darüber Verfügungsbefugten unterfertigte Erklärung anzuschließen, dass er dem Auftraggeber die Datenbestände für die Untersuchung zur Verfügung stellt. Anstelle dieser Erklärung kann auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 der Exekutionsordnung – EO, RGBl. Nr. 79/1896) vorgelegt werden.

(4) Rechtliche Beschränkungen der Zulässigkeit der Benützung von Daten aus anderen, insbesondere urheberrechtlichen Gründen bleiben unberührt.

(5) Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personsbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personsbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

§ 47. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adreßdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung der Zustimmung der Betroffenen.

(2) Wenn allerdings angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung eine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist, bedarf es keiner Zustimmung, wenn

1. Daten desselben Auftraggebers verwendet werden oder
2. bei einer beabsichtigten Übermittlung der Adreßdaten an Dritte
 - a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
 - b) der Betroffene nach entsprechender Information über Anlaß und Inhalt der Übermittlung innerhalb angemessener Frist keinen Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der Zustimmung der Betroffenen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adreßdaten mit Genehmigung der Datenschutzkommission gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst oder
2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder
3. zur Befragung der Betroffenen für wissenschaftliche oder statistische Zwecke erfolgen soll.

(4) Die Datenschutzkommission hat auf Antrag eines Auftraggebers, der Adressdaten verarbeitet, die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht

und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.

(5) Die übermittelten Adreßdaten dürfen ausschließlich für den genehmigten Zweck verwendet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) In jenen Fällen, in welchen es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adreßdaten notwendigen Verarbeitungen vorgenommen werden.

Publizistische Tätigkeit

§ 48. (1) Soweit Medienunternehmen, Mediendienste oder ihre Mitarbeiter Daten unmittelbar für ihre publizistische Tätigkeit im Sinne des Mediengesetzes verwenden, sind von den einfachgesetzlichen Bestimmungen des vorliegenden Bundesgesetzes nur die §§ 4 bis 6, 10, 11, 14 und 15 anzuwenden.

(2) Die Verwendung von Daten für Tätigkeiten nach Abs. 1 ist insoweit zulässig, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihrer Mitarbeiter in Ausübung des Grundrechtes auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK erforderlich ist.

(3) Im übrigen gelten die Bestimmungen des Mediengesetzes, insbesondere seines dritten Abschnitts über den Persönlichkeitsschutz.

Verwendung von Daten im Katastrophenfall

§ 48a. (1) Auftraggeber des öffentlichen Bereiches sind im Katastrophenfall ermächtigt, Daten zu verwenden, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängern und Verstorbenen und zur Information von Angehörigen notwendig ist. Zu diesem Zweck sind auch Hilfsorganisationen (Abs. 6) nach Maßgabe der ihnen zukommenden Aufgaben und rechtlichen Befugnis ermächtigt, Daten zu verwenden. Wenn dies zur raschen Bewältigung der Katastrophe notwendig ist, darf eine Datenverwendung in Form der Teilnahme an einem Informationsverbundsystem erfolgen. Wer rechtmäßig über Daten verfügt, darf diese an Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen übermitteln, sofern diese die Daten zur Bewältigung der Katastrophe für die genannten Zwecke benötigen. Die Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.

(2) Eine Überlassung oder Übermittlung von Daten in das Ausland ist zulässig, soweit dies für die Erfüllung der in Abs. 1 genannten Zwecke notwendig ist. Wenn dies zur raschen Bewältigung der Katastrophe notwendig ist, darf eine Datenverwendung durch Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen in Form der Teilnahme an einem Informationsverbundsystem, an dem auch ausländische Auftraggeber beteiligt sind, erfolgen. Die Übermittlung erkennungsdienstlicher und sensibler Daten zu Identifizierungszwecken an ein derartiges System darf erst stattfinden, wenn auf Grund von Erhebungen konkrete Anhaltspunkte dafür vorliegen, dass die vermisste Person verstorben sein dürfte. Daten, die für sich allein den Betroffenen strafrechtlich belasten, dürfen nicht übermittelt werden, es sei denn, dass diese zur Identifizierung im Einzelfall unbedingt notwendig sind. Die Übermittlung von Daten Angehöriger darf nur in pseudonymisierter Form erfolgen. Daten dürfen in Staaten ohne angemessenes Datenschutzniveau nur übermittelt oder überlassen werden, wenn der Auftraggeber auf Grund schriftlicher Vereinbarungen mit dem Empfänger oder auf Grund schriftlicher Zusagen des Empfängers oder, wenn dies nach den Umständen nicht oder nicht in angemessener Zeit möglich ist, durch Erteilung von Auflagen an den Empfänger davon ausgehen kann, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Eine Übermittlung oder Überlassung hat dann zu unterbleiben, wenn Grund zur Annahme besteht, dass der Empfänger nicht für den gebotenen Schutz der Geheimhaltungsinteressen der Betroffenen Sorge tragen oder ausdrückliche datenschutzrechtliche Auflagen des Auftraggebers missachten werde. Während der Dauer der Katastrophensituation entfällt im Hinblick auf § 12 Abs. 3 Z 3 die Genehmigungspflicht. Die Datenschutzkommission ist von den veranlassten Übermittlungen und Überlassungen und den näheren Umständen des Anlass gebenden Sachverhaltes jedoch unverzüglich zu verständigen. Die Datenschutzkommission kann zum Schutz der Betroffenenrechte Datenübermittlungen oder -überlassungen untersagen, wenn der durch die Datenweitergabe bewirkte Eingriff in das Grundrecht auf Datenschutz durch die besonderen Umstände der Katastrophensituation nicht gerechtfertigt ist.

(3) Auf Grund einer konkreten Anfrage eines nahen Angehörigen einer tatsächlich oder vermutlich von der Katastrophe unmittelbar betroffenen Person sind Auftraggeber ermächtigt, dem Anfragenden Daten über die Reise in das und aus dem Katastrophengebiet, Aufenthaltsdaten im Katastrophengebiet sowie Daten über den Stand der Ausforschung von betroffenen Personen zu übermitteln, wenn der Angehörige folgende Daten bekannt gibt:

1. Vor- und Zuname, Geburtsdatum sowie Wohnadresse der tatsächlich oder vermutlich von der Katastrophe betroffenen Person und
 2. seinen Vor- und Zunamen, sein Geburtsdatum, seine Wohnadresse und sonstige Erreichbarkeit sowie seine Angehörigeneigenschaft zur betroffenen Person.
- Bestehen Zweifel an der Angehörigeneigenschaft und können diese durch Überprüfungen nicht ausgeräumt werden, ist ein Nachweis der Identität und Angehörigeneigenschaft notwendig.

(4) Über Abs. 3 hinaus dürfen nahen Angehörigen von Auftraggebern des öffentlichen Bereiches und Hilfsorganisationen Daten einschließlich sensibler Daten über tatsächlich oder vermutlich unmittelbar von der Katastrophe betroffene Personen nur übermittelt werden, wenn sie ihre Identität und ihre Angehörigeneigenschaft nachweisen und die Auskunft zur Wahrung ihrer

Rechte oder jener der betroffenen Person erforderlich ist. Die Sozialversicherungsträger sind verpflichtet, die Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen bei der Überprüfung der Daten gemäß Abs. 3 und der Angehörigenbeziehung zu unterstützen. Behörden sind ermächtigt, die zur Überprüfung dieser Angaben notwendigen Daten im Wege der Amtshilfe zu ermitteln und für diesen Zweck zu verwenden.

(5) Als nahe Angehörige im Sinne dieser Bestimmung sind Eltern, Kinder, Ehegatten, eingetragene Partner und Lebensgefährten der Betroffenen zu verstehen. Andere Angehörige dürfen die erwähnten Auskünfte unter denselben Voraussetzungen wie nahe Angehörige dann erhalten, wenn sie eine besondere Nahebeziehung zu der von der Katastrophe tatsächlich oder vermutlich unmittelbar betroffenen Person glaubhaft machen.

(6) Eine Hilfsorganisation im Sinne dieser Bestimmung ist eine allgemein anerkannte gemeinnützige Organisation, die statuten- oder satzungsgemäß das Ziel hat, Menschen in Notsituationen zu unterstützen und von der angenommen werden kann, dass sie in wesentlichem Ausmaß eine Hilfeleistung im Katastrophenfall erbringen kann.

(7) Alle Datenverwendungen sind im Sinne des § 14 Abs. 2 Z 7 zu protokollieren.

(8) Die Zulässigkeit von Datenverwendungen auf der Grundlage anderer in den §§ 8 und 9 genannter Tatbestände bleibt unberührt.

9. Abschnitt Besondere Verwendungsarten von Daten

Automatisierte Einzelentscheidungen

§ 49. (1) Niemand darf einer für ihn rechtliche Folgen nach sich ziehenden oder einer ihn erheblich beeinträchtigenden Entscheidung unterworfen werden, die ausschließlich auf Grund einer automationsunterstützten Verarbeitung von Daten zum Zweck der Bewertung einzelner Aspekte seiner Person ergeht, wie beispielsweise seiner beruflichen Leistungsfähigkeit, seiner Kreditwürdigkeit, seiner Zuverlässigkeit oder seines Verhaltens.

(2) Abweichend von Abs. 1 darf eine Person einer ausschließlich automationsunterstützt erzeugten Entscheidung unterworfen werden, wenn

1. dies gesetzlich ausdrücklich vorgesehen ist oder
2. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages ergeht und dem Ersuchen des Betroffenen auf Abschluß oder Erfüllung des Vertrages stattgegeben wurde oder
3. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen - beispielsweise die Möglichkeit, seinen Standpunkt geltend zu machen - garantiert wird.

(3) Dem Betroffenen ist bei automatisierten Einzelentscheidungen auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen. § 26 Abs. 2 bis 10 gilt sinngemäß.

Informationsverbundsysteme

§ 50. (1) Die Auftraggeber eines Informationsverbundsystems haben, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen. Name (Bezeichnung) und Anschrift des Betreibers sind in der Meldung zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet des Rechtes des Betroffenen auf Auskunft nach § 26 hat der Betreiber jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen; in Fällen, in welchen der Auftraggeber gemäß § 26 Abs. 5 vorzugehen hätte, hat der Betreiber mitzuteilen, daß kein der Pflicht zur Auskunftserteilung unterliegender Auftraggeber benannt werden kann. Abgesehen von der abweichenden Frist gilt § 26 Abs. 3 bis 10 sinngemäß. Die Unterstützungspflicht des Betreibers gilt auch bei Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber unter den gleichen Voraussetzungen, wie sie in § 33 Abs. 3 vorgesehen sind, befreien. Wird ein Informationsverbundsystem geführt, ohne daß eine entsprechende Meldung an die Datenschutzkommission unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.

(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten, insbesondere auch die Vornahme der Meldung des Informationsverbundsystems, auf den Betreiber übertragen werden. Allein für die Übertragung der Meldepflicht ist die Vorlage von Vollmachten nach § 10 AVG nicht erforderlich. Soweit der Pflichtenübergang nicht durch Gesetz angeordnet ist, ist er gegenüber Dritten nur wirksam, wenn er – auf Grund einer entsprechenden Meldung an die Datenschutzkommission – aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.

(2a) Wird ein Informationsverbundsystem auf Grund einer Meldung von zumindest zwei Auftraggebern registriert, so können Auftraggeber, die in der Folge die Teilnahme an dem Informationsverbundsystem anstreben, die Meldung im Umfang des § 19 Abs. 1 Z 3 bis 7 auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken, wenn sie eine Teilnahme im genau gleichen Umfang anstreben.

(3) Die Bestimmungen der Abs. 1 und 2 gelten nicht, soweit infolge der besonderen, insbesondere internationalen Struktur eines bestimmten Informationsverbundsystems gesetzlich ausdrücklich anderes vorgesehen ist.

9a.Abschnitt Videoüberwachung

Allgemeines

§ 50a. (1) Videoüberwachung im Sinne dieses Abschnittes bezeichnet die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte. Für derartige Überwachungen gelten die folgenden Absätze, sofern nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Für Videoüberwachung gelten die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3). Rechtmäßige Zwecke einer Videoüberwachung, insbesondere der Auswertung und Übermittlung der dabei ermittelten Daten, sind jedoch vorbehaltlich des Abs. 5 nur der Schutz des überwachten Objekts oder der überwachten Person oder die Erfüllung rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, im Hinblick auf Ereignisse nach Abs. 1. Persönlichkeitsrechte nach § 16 ABGB bleiben unberührt.

(3) Ein Betroffener ist durch eine Videoüberwachung dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn

1. diese im lebenswichtigen Interesse einer Person erfolgt, oder
2. Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder
3. er der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.

(4) Ein Betroffener ist darüber hinaus durch eine Videoüberwachung ausschließlich dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn sie nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgt und

1. bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden, oder
2. unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der überwachten Person auferlegen, oder
3. sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden (Echtzeitüberwachung), und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

(5) Mit einer Videoüberwachung nach Abs. 4 dürfen nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen. Weiters ist die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt.

(6) Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 bis 4 hinaus in folgenden Fällen übermittelt werden:

1. an die zuständige Behörde oder das zuständige Gericht, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder
2. an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs. 5 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, eingeräumten Befugnisse, auch wenn sich die Handlung oder der Angriff nicht gegen das überwachte Objekt oder die überwachte Person richtet. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Auftraggebers bleiben unberührt.

(7) Mit einer Videoüberwachung gewonnene Daten von Betroffenen dürfen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.

Besondere Protokollierungs- und Löschungspflicht

§ 50b. (1) Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren. Dies gilt nicht für Fälle der Echtzeitüberwachung.

(2) Aufgezeichnete Daten sind, sofern sie nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- oder Beweissicherungszwecke oder für Zwecke nach § 50a Abs. 6 benötigt werden, spätestens nach 72 Stunden zu löschen. § 33 Abs. 2 AVG gilt. Eine beabsichtigte längere Aufbewahrungsdauer ist in der Meldung anzuführen und zu begründen. In diesem Fall darf die Datenschutzkommission die Videoüberwachung nur registrieren, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist.

Meldepflicht und Registrierungsverfahren

§ 50c. (1) Videoüberwachungen unterliegen der Meldepflicht gemäß den §§ 17 ff. Sofern der Auftraggeber nicht in der Meldung zusagt, die Videoüberwachungsdaten zu verschlüsseln und unter Hinterlegung des einzigen Schlüssels bei der Datenschutzkommission sicherzustellen, dass eine Auswertung der Videoaufzeichnungen nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet, unterliegen sie der Vorabkontrolle (§ 18 Abs. 2). Bestimmte Tatsachen im Sinn von § 50a Abs. 4 Z 1 müssen bei Erstattung der Meldung glaubhaft gemacht werden. Soweit gemäß § 96a des Arbeitsverfassungsgesetzes 1974 – ArbVG, BGBl. Nr. 22, Betriebsvereinbarungen abzuschließen sind, sind diese im Registrierungsverfahren vorzulegen.

(2) Eine Videoüberwachung ist über § 17 Abs. 2 und 3 hinaus von der Meldepflicht ausgenommen

1. in Fällen der Echtzeitüberwachung oder

2. wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.

(3) Mehrere überwachte Objekte oder überwachte Personen, für deren Videoüberwachung derselbe Auftraggeber eine gesetzliche Zuständigkeit oder rechtliche Befugnis (§ 7 Abs. 1) hat, können auf Grund ihrer gleichartigen Beschaffenheit oder ihrer räumlichen Verbundenheit in einer Meldung zusammengefasst werden, wenn sich diese auf die gleiche Rechtsgrundlage stützt.

Information durch Kennzeichnung

§ 50d. (1) Der Auftraggeber einer Videoüberwachung hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Auftraggeber eindeutig hervorzugehen, es sei denn, dieser ist den Betroffenen nach den Umständen des Falles bereits bekannt. Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

(2) Keine Kennzeichnungsverpflichtung besteht bei Videoüberwachungen im Rahmen der Vollziehung hoheitlicher Aufgaben, die nach § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

Auskunftsrecht

§ 50e. (1) Abweichend von § 26 Abs. 1 ist dem Auskunftswerber, nachdem dieser den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, und den Ort möglichst genau benannt und seine Identität in geeigneter Form nachgewiesen hat, Auskunft über die zu seiner Person verarbeiteten Daten durch Übersendung einer Kopie der zu seiner Person verarbeiteten Daten in einem üblichen technischen Format zu gewähren. Alternativ kann der Auskunftswerber eine Einsichtnahme auf Lesegeräten des Auftraggebers verlangen, wobei ihm auch in diesem Fall die Ausfolgung einer Kopie zusteht. Die übrigen Bestandteile der Auskunft (verfügbare Informationen über die Herkunft, Empfänger oder Empfängerkreise von Übermittlungen, Zweck, Rechtsgrundlagen sowie allenfalls Dienstleister) sind auch im Fall der Überwachung schriftlich zu erteilen, wenn nicht der Auskunftswerber einer mündlichen Auskunftserteilung zustimmt.

(2) § 26 Abs. 2 ist mit der Maßgabe anzuwenden, dass in dem Fall, dass eine Auskunft wegen überwiegender berechtigter Interessen Dritter oder des Auftraggebers nicht in der in Abs. 1 geregelten Form erteilt werden kann, der Auskunftswerber Anspruch auf eine schriftliche Beschreibung seines von der Überwachung verarbeiteten Verhaltens oder auf eine Auskunft unter Unkenntlichmachung der anderen Personen hat.

(3) In Fällen der Echtzeitüberwachung ist ein Auskunftsrecht ausgeschlossen.

10. Abschnitt Strafbestimmungen

Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

Verwaltungsstrafbestimmung

§ 52. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 25.000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder
4. Daten vorsätzlich entgegen § 26 Abs. 7 löscht;
5. sich unter Vortäuschung falscher Tatsachen vorsätzlich Daten gemäß § 48a verschafft.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 10.000 Euro zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß den §§ 17 oder 50c erfüllt zu haben oder eine Datenanwendung auf eine von der Meldung abweichende Weise betreibt oder
2. Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 Abs. 1 eingeholt zu haben oder
3. gegen gemäß § 13 Abs. 2 Z 2, § 19 oder § 50c Abs. 1 abgegebene Zusagen oder von der Datenschutzkommission gemäß § 13 Abs. 1 oder § 21 Abs. 2 erteilte Auflagen verstößt oder
4. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24, 25 oder 50d verletzt oder
5. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht lässt oder
6. die gemäß § 50a Abs. 7 und § 50b Abs. 1 erforderlichen Sicherheitsmaßnahmen außer Acht lässt oder
7. Daten nach Ablauf der in § 50b Abs. 2 vorgesehene Lösungsfrist nicht löscht.

(2a) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit einer Strafe bis zu 500 Euro zu ahnden ist, wer Daten entgegen den §§ 26, 27 oder 28 nicht fristgerecht beauskunftet, richtigstellt oder löscht.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

(5) Zuständig für Entscheidungen nach Abs. 1 bis 4 ist die Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat. Falls ein solcher im Inland nicht gegeben ist, ist die am Sitz der Datenschutzkommission eingerichtete Bezirksverwaltungsbehörde zuständig.

11. Abschnitt Übergangs- und Schlußbestimmungen

Befreiung von Gebühren, Abgaben und vom Kostenersatz

§ 53. (1) Die durch dieses Bundesgesetz unmittelbar veranlaßten Eingaben der Betroffenen zur Wahrung ihrer Interessen sowie die Eingaben im Registrierungsverfahren und die gemäß § 21 Abs. 3 zu erstellenden Registerauszüge sind von den Stempelgebühren und von den Verwaltungsabgaben des Bundes befreit.

(2) Für Abschriften aus dem Datenverarbeitungsregister, die ein Betroffener zur Verfolgung seiner Rechte benötigt, ist kein Kostenersatz zu verlangen.

§ 54. (1) Von der Erlassung eines Bundesgesetzes, das die Zulässigkeit der Verarbeitung sensibler Daten betrifft, hat der Bundeskanzler anlässlich der Kundmachung des Gesetzes im Bundesgesetzblatt der Europäischen Kommission Mitteilung zu machen.

(2) Die Datenschutzkommission hat den anderen Mitgliedstaaten der Europäischen Union und der Europäischen Kommission mitzuteilen, in welchen Fällen

1. keine Genehmigung für den Datenverkehr in ein Drittland erteilt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 1 nicht als gegeben erachtet wurden;
2. der Datenverkehr in ein Drittland ohne angemessenes Datenschutzniveau genehmigt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 2 als gegeben erachtet wurden.

Feststellungen der Europäischen Kommission

§ 55. Der Inhalt der in einem Verfahren gemäß Art. 31 Abs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31, getroffenen Feststellungen der Europäischen Kommission über

1. das Vorliegen oder Nichtvorliegen eines angemessenen Datenschutzniveaus in einem Drittland oder
2. die Eignung bestimmter Standardvertragsklauseln oder Verpflichtungserklärungen zur Gewährleistung eines ausreichenden Schutzes der Datenverwendung in einem Drittland ist vom Bundeskanzler im Bundesgesetzblatt gemäß § 4 des Bundesgesetzblattgesetzes, BGBl. I Nr. 100/2003, kundzumachen.

Verwaltungsangelegenheiten gemäß Art. 30 B-VG

§ 56. Der Präsident des Nationalrats ist Auftraggeber jener Datenanwendungen, die für Zwecke der ihm gemäß Art. 30 B-VG übertragenen Angelegenheiten durchgeführt werden. Übermittlungen von Daten aus solchen Datenanwendungen dürfen nur über Auftrag des Präsidenten des Nationalrats vorgenommen werden. Der Präsident trifft Vorsorge dafür, daß im Falle eines Übermittlungsauftrags die Voraussetzungen des § 7 Abs. 2 vorliegen und insbesondere die Zustimmung des Betroffenen in jenen Fällen eingeholt wird, in welchen dies gemäß § 7 Abs. 2 mangels einer anderen Rechtsgrundlage für die Übermittlung notwendig ist.

Sprachliche Gleichbehandlung

§ 57. Soweit in diesem Artikel auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

Manuelle Dateien

§ 58. Soweit manuell, dh. ohne Automationsunterstützung geführte Dateien für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenanwendungen im Sinne des § 4 Z 7. § 17 gilt mit der Maßgabe, daß die Meldepflicht nur für solche Dateien besteht, deren Inhalt gemäß § 18 Abs. 2 der Vorabkontrolle unterliegt.

Umsetzungshinweis

§ 59. Mit diesem Bundesgesetz wird die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31, umgesetzt.

Inkrafttreten

§ 60. (1) (Anm.: Durch Art. 2 § 2 Abs. 1 Z 24 und Abs. 2 Z 71, BGBl. I Nr. 2/2008, als nicht mehr geltend festgestellt.)

(2) Die übrigen Bestimmungen dieses Bundesgesetzes treten ebenfalls mit 1. Jänner 2000 in Kraft.

(3) §§ 26 Abs. 6 und 52 Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 136/2001 treten mit 1. Jänner 2002 in Kraft.

(4) § 48a Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. 135/2009 tritt mit 1. Jänner 2010 in Kraft.



(5) Das Inhaltsverzeichnis, § 4 Abs. 1 Z 4, 5, 7 bis 9, 11 und 12, § 8 Abs. 1, 2 und 4, § 12 Abs. 1, die Umnummerierung der Absätze in § 13, § 16 Abs. 1 und 3, § 17 Abs. 1, 1a und 4, § 19 Abs. 1 Z 3a und Abs. 2, die Umnummerierung der Absätze in § 19, die §§ 20 bis 22a samt Überschriften, § 24 Abs. 2a, § 24 Abs. 4, § 26 Abs. 1 bis 8 und 10, § 28 Abs. 3, § 30 Abs. 2a, 5 bis 6a, die §§ 31 und 31a samt Überschriften, § 32 Abs. 1, 4, 6 und 7, § 34 Abs. 1, 3 und 4, § 36 Abs. 3, 3a und 9, § 39 Abs. 5, § 40 Abs. 1 und 2, § 41 Abs. 2 Z 4a, § 42 Abs. 1 Z 1, § 42 Abs. 5, § 46 Abs. 1 Z 2 und 3, Abs. 2 bis 3a, § 47 Abs. 4, § 49 Abs. 3, § 50 Abs. 1 bis 2a, der 9a. Abschnitt, § 51, § 52 Abs. 2 und 4, § 55, § 61 Abs. 6 bis 9 sowie § 64 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 treten mit 1. Jänner 2010 in Kraft. Gleichzeitig treten § 4 Abs. 1 Z 10, § 13 Abs. 3 sowie § 51 Abs. 2 außer Kraft.

(6) § 36 Abs. 6 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 tritt am 1. Juli 2010 in Kraft.

Abs. 4: Verfassungsbestimmung Übergangsbestimmungen

§ 61. (1) Meldungen, die vor Inkrafttreten dieses Bundesgesetzes an das Datenverarbeitungsregister erstattet wurden, gelten als Meldungen im Sinne des § 17, soweit sie nicht im Hinblick auf das Entfallen von Meldepflichten gemäß § 17 Abs. 2 oder 3 gegenstandslos geworden sind. Desgleichen gelten vor Inkrafttreten dieses Bundesgesetzes durchgeführte Registrierungen als Registrierungen im Sinne des § 21.

(2) Soweit nach der neuen Rechtslage eine Genehmigung für die Übermittlung von Daten ins Ausland erforderlich ist, muß für Übermittlungen, für die eine Genehmigung vor Inkrafttreten dieses Bundesgesetzes erteilt wurde, eine Genehmigung vor dem 1. Jänner 2003 neu beantragt werden. Wird der Antrag rechtzeitig gestellt, dürfen solche Übermittlungen bis zur rechtskräftigen Entscheidung über den Genehmigungsantrag fortgeführt werden.

(3) Datenschutzverletzungen, die vor dem Inkrafttreten dieses Bundesgesetzes stattgefunden haben, sind, soweit es sich um die Feststellung der Rechtmäßigkeit oder Rechtswidrigkeit eines Sachverhalts handelt, nach der Rechtslage zum Zeitpunkt der Verwirklichung des Sachverhalts zu beurteilen; soweit es sich um die Verpflichtung zu einer Leistung oder Unterlassung handelt, ist die Rechtslage im Zeitpunkt der Entscheidung in erster Instanz zugrunde zu legen. Ein strafbarer Tatbestand ist nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist; dies gilt auch für das Rechtsmittelverfahren.

(4) (Verfassungsbestimmung) Datenanwendungen, die für die in § 17 Abs. 3 genannten Zwecke notwendig sind, dürfen auch bei Fehlen einer im Sinne des § 1 Abs. 2 ausreichenden gesetzlichen Grundlage bis 31. Dezember 2007 vorgenommen werden, in den Fällen des § 17 Abs. 3 Z 1 bis 3 jedoch bis zur Erlassung von bundesgesetzlichen Regelungen über die Aufgaben und Befugnisse in diesen Bereichen.

(5) Manuelle Datenanwendungen, die gemäß § 58 der Meldepflicht unterliegen, sind, soweit sie schon im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bestanden haben, dem Datenverarbeitungsregister bis spätestens 1. Jänner 2003 zu melden. Dasselbe gilt für automationsunterstützte Datenanwendungen gemäß § 17 Abs. 3, für die durch die nunmehr geltende Rechtslage die Meldepflicht neu eingeführt wurde.

(6) Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, bleiben in ihrer registrierten Form rechtmäßig, wenn sie den am 31. Dezember 2009 geltenden datenschutzrechtlichen Bestimmungen genügen und die Datenschutzkommission keine Befristung verfügt hat. Hat die Datenschutzkommission hingegen eine Befristung einer solchen Videoüberwachung verfügt, bleibt diese bis zum Ablauf der Befristung, längstens aber bis zum 31. Dezember 2012 rechtmäßig.

(7) Soweit in einzelnen Vorschriften Verweise auf das Datenschutzgesetz, BGBl. Nr. 565/1978, enthalten sind, gelten diese bis zu ihrer Anpassung an dieses Bundesgesetz sinngemäß weiter.

(8) Die Verordnung nach § 16 Abs. 3 ist vom Bundeskanzler nach Maßgabe der technischen Möglichkeiten des Datenverarbeitungsregisters bis spätestens 1. September 2012 neu zu erlassen. Bis zum Inkrafttreten dieser Verordnung sind die §§ 16 bis 22, § 30 Abs. 3 und 6 sowie § 40 Abs. 1 (letzterer mit Ausnahme des Verweises auf § 31a Abs. 3) in der Fassung vor dem Bundesgesetz BGBl. I Nr. 133/2009 anzuwenden; § 22a, § 30 Abs. 2a und 6a, § 31a Abs. 1 und 2 sowie § 32 Abs. 7 sind bis dahin nicht anzuwenden. § 31 Abs. 3 in der Fassung vor dem Bundesgesetz BGBl. I Nr. 133/2009 ist bis dahin zusätzlich weiter anzuwenden. Die Erklärung, ob eine Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 genannten Tatbestände erfüllt (§ 19 Abs. 1 Z 3a), ist der Datenschutzkommission bei im Zeitpunkt des Inkrafttretens der neuen Verordnung nach § 16 Abs. 3 registrierten Datenanwendungen anlässlich der ersten über eine Streichung hinausgehenden Änderungsanmeldung zu melden, die nach diesem Zeitpunkt erstattet wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 3a ist nicht erforderlich.

Verordnungserlassung

§ 62. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

Verweisungen

§ 63. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollziehung

§ 64. Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung obliegt, der Bundeskanzler und die anderen Bundesminister im Rahmen ihres Wirkungsbereiches betraut.

Wer darf was?

Auszug aus dem Österreichischen Datenschutzgesetz 2000

Besondere Verwendungszwecke von Daten

Private Zwecke

§45. (1) Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten verarbeiten, wenn sie ihnen vom Betroffenen selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise, insbesondere in Übereinstimmung mit §7 Abs.2, zugekommen sind.

(2) Daten, die eine natürliche Person für ausschließlich persönliche oder familiäre Tätigkeiten verarbeitet, dürfen, soweit gesetzlich nicht ausdrücklich anderes vorgesehen ist, für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.

Wissenschaftliche Forschung und Statistik

§46. (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die

1. öffentlich zugänglich sind oder
2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für ihn nur indirekt personenbezogen sind.

Andere Daten dürfen nur unter den Voraussetzungen des Abs.2 Z 1 bis 3 verwendet werden.

(2) Bei Datenanwendungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs.1 fallen, dürfen Daten nur

1. gemäß besonderen gesetzlichen Vorschriften oder
2. mit Zustimmung des Betroffenen oder
3. mit Genehmigung der Datenschutzkommission gemäß Abs.3 verwendet werden.

(...)

(4) Rechtliche Beschränkungen der Zulässigkeit der Benützung von Daten aus anderen, insbesondere urheberrechtlichen Gründen bleiben unberührt.

(5) Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personsbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personsbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

§47. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adreßdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung der Zustimmung der Betroffenen.

(2) Wenn allerdings angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung eine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist, bedarf es keiner Zustimmung, wenn

1. Daten desselben Auftraggebers verwendet werden oder
2. bei einer beabsichtigten Übermittlung der Adreßdaten an Dritte
 - a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
 - b) der Betroffene nach entsprechender Information über Anlaß und Inhalt der Übermittlung innerhalb angemessener Frist keinen Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs.2 nicht vor und würde die Einholung der Zustimmung der Betroffenen gemäß Abs.1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adreßdaten mit Genehmigung der Datenschutzkommission gemäß Abs.4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst oder
2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder
3. zur Befragung der Betroffenen für wissenschaftliche oder statistische Zwecke erfolgen soll.

(...)

(5) Die übermittelten Adreßdaten dürfen ausschließlich für den genehmigten Zweck verwendet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) In jenen Fällen, in welchen es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adreßdaten notwendigen Verarbeitungen vorgenommen werden.

**Endlich 80!**

Margit N. organisiert die Geburtstagsfeier zum 80er ihrer Oma. Zu dem Fest sind alle Verwandten eingeladen, auch jene, zu denen sie sonst wenig Kontakt hat. Schon lange vor dem Fest ruft Margit alle, die eingeladen werden sollen, an, und fragt nach deren Adressen und E-Mail-Adressen, um die offiziellen Einladungen verschicken zu können. Außerdem bittet sie um Bekanntgabe der Handynummern, um die Eingeladenen im Bedarfsfall möglichst rasch erreichen zu können. So entsteht eine ansehnliche Kontaktliste ihrer Verwandten. Eine Woche vor dem Fest beschließt Margit, alle

Gäste sicherheitshalber nochmals telefonisch zu kontaktieren. Damit es schneller geht, teilt sie sich diese Aufgabe mit ihrer Schwester.

- ☐ Ja, ist laut Österreichischem Datenschutzgesetz erlaubt.
☐ Nein, ist laut Österreichischem Datenschutzgesetz verboten.

Begründung:

.....

.....

.....

.....

**Spitzenangebot zum Freundes-Sonderpreis**

Bernd P. ist zu einer großen Geburtstagsfeier eingeladen. Die letzten Informationen zum Ablauf des Festes bekommt er per E-Mail, das mit offenem Verteiler verschickt wird. Nachdem Bernd P. als Versicherungsvertreter arbeitet, nutzt er die Gelegenheit und verwendet diese Adressen, um allen Gästen der Geburtstagsfeier ein Angebot für eine private Pensionsvorsorge zu schicken.

- ☐ Ja, ist laut Österreichischem Datenschutzgesetz erlaubt.
☐ Nein, ist laut Österreichischem Datenschutzgesetz verboten.

Begründung:

.....

.....

.....

.....



Informationen aus erster Hand

Die Studentin Nadine H. schreibt eine Seminararbeit, für die sie „Feldforschung“ betreibt. Zum Thema „Das Radio und seine Bedeutung in den 70er Jahren des 20. Jahrhunderts“ erstellt sie einen Fragebogen, den sie an verschiedenste Personen über 60 verteilt, die sich bereit erklärt haben, an ihrer Befragung teilzunehmen. Damit Nadine H. die Ergebnisse hinsichtlich verschiedenster Kriterien auswerten kann, geben die Befragten auch Daten wie Alter, Geschlecht und Familienstand an. Schlussendlich werden die Ergebnisse anonymisiert, das heißt, dass aus der Seminararbeit

nicht ersichtlich ist, welche Personen befragt wurden und wer welche Antwort gegeben hat. Zwei Semester später verwendet Nadine die Ergebnisse dieser Umfrage für eine andere Arbeit, bei der es um die Scheidungsrate der Generation 60+ geht. Auch diesmal erfolgt die Auswertung anonym.

- ☐ Ja, ist laut Österreichischem Datenschutzgesetz erlaubt.
- ☐ Nein, ist laut Österreichischem Datenschutzgesetz verboten.

Begründung:

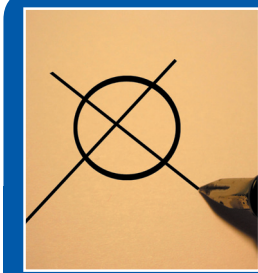


Forschen leicht gemacht!

Bernhard E. studiert an der Uni Wien und soll eine Forschungsarbeit über die Lebensumstände von Männern über 65 Jahren schreiben. Nachdem er weiß, dass seine Uni-Kollegin Nadine H. bereits in einem anderen Zusammenhang Interviews mit vielen Personen dieser Altersgruppe geführt hat, bittet er sie um die Liste ihrer Interviewpartner, um alle Männer auf der Liste anzurufen und nachzufragen, ob er sie zu seinem Thema interviewen darf. Nadine H. weiß, wie schwierig es gewesen ist, Freiwillige für ihre Befragung zu finden, und händigt Bernhard E. die Liste bereitwillig aus.

- ☐ Ja, ist laut Österreichischem Datenschutzgesetz erlaubt.
- ☐ Nein, ist laut Österreichischem Datenschutzgesetz verboten.

Begründung:

**Zeit zum Wählen?**

Sandra S. feiert zwei Tage vor den Nationalratswahlen ihren 16. Geburtstag. Das heißt, sie darf zum ersten Mal wählen gehen. Drei Wochen vor der Wahl erhält sie einen persönlich an sie adressierten Brief, der eine von der Nationalratspräsidentin herausgegebene Infobroschüre enthält, die über die Aufgaben des Nationalrates informiert und Sandra daran erinnert und dazu auffordert, bei der nächsten Wahl von ihrem Stimmrecht Gebrauch zu machen.

- ☐ Ja, ist laut Österreichischem Datenschutzgesetz erlaubt.
- ☐ Nein, ist laut Österreichischem Datenschutzgesetz verboten.

Begründung:



Meine Daten im Ausverkauf?

Ich nehme immer wieder an Gewinnspielen teil. Dass ich dabei auch ein paar Daten von mir bekannt geben muss, ist ja wohl klar – immerhin müssen die Organisatoren des Gewinnspiels ja auch wissen, wem sie im Fall der Fälle die frohe Gewinnbotschaft überbringen dürfen!



Ich mache immer wieder bei Markt- und Meinungsumfragen mit. Oft bekommt man dafür auch Produkte geschenkt, manchmal gibt's sogar ein bisschen Geld. Klar, dass ich dann nicht nur mein Alter und meine Adresse, sondern auch persönlichere Details bekanntgebe! Sonst macht das Ganze ja keinen Sinn!

Ich liebe und sammle Kundenkarten! Die Spezialangebote, bei denen man damit zuschlagen kann, finde ich einfach toll! Da macht Einkaufen gleich viel mehr Spaß!



Ich beteilige mich immer wieder an Diskussionen in Internetforen. Manchmal zu ganz unwichtigen Themen, aber zwischendurch geht's auch zu echt wichtigen Themen richtig heiß her! Nachdem ich keinen Grund dazu sehe, nicht zu meiner Meinung zu stehen, gebe ich schon aus Prinzip immer meinen richtigen Namen und meine vollständigen Kontaktdaten an.

Immer mehr Lokale informieren mittlerweile via SMS über ihr Programm. Find ich echt super – so bin ich immer up to date. Mein Handy habe ich immer bei mir, bei meinen Mails kann's schon mal vorkommen, dass ich sie ein oder zwei Tage nicht abfrage. Wäre doch jammerschade, wenn ich deswegen einen angesagten Event versäumen würde!





Datenproduzent Handy

Verkehrsdaten



Stammdaten



Standortdaten



Inhaltsdaten



109

Richtig kombiniert?

Verbinde die richtigen Satzteile!

Wenn jemand weiß, mit wem du telefonierst,

Wer über die zeitliche Nutzung deines Handys
Bescheid weiß,

Wie oft und wie lang du mit jemandem telefonierst,

Wo du den lieben langen Tag unterwegs bist,

Die Verkehrs- und Standortdaten deines Telefons

kann man aus den Standortdaten deines Handys
ablesen.

kann er daraus auf deinen Freundes- und
Bekanntenzirkel schließen.

verraten nichts über Gesprächs- oder
Nachrichteninhalte.

ist auch über deinen Tagesablauf informiert.

zeigt, wie wichtig dir diese Person ist.

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 Auskunftsbegehens.

(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 beansprucht 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.



© babimu - Fotolia.com

Smart & Safe

FMK
FORUM MOBILKOMMUNIKATION

	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.			

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.

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 Mobilfunkgeräteerkennung (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?

.....

.....





Pro & Kontra



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

+	-



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 verdächtige 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 Rechtferti-

gungsnotstand kommen, nur weil sie einem Freund den Zwischenstand durchgegeben haben, fürchtet Zeger - und der Gegenbeweis, mit Randalen 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 Benutzer - ins Internet einklinkt. Wieder ein Beispiel von der Arge Daten: Die Polizei sucht den Urheber einer Drohbotschaft, die von einer bestimmten IP-Adresse ausgesandt 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 Teilnehmerken-

nung 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 Teilnehmererkennung 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 Informationsbegehrt 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 Informationsbegehrt 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.

Datenschutzler 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 Strafbzahlungen 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 Unterstützungserklärungen erhalten zu haben, um gegen die Vorratsdatenspeicherung vorzugehen. Konkret wer-

den 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 Telefonnummer 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 Rechtsschutzbeauftragten 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 Officialdelikt 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 be-

rappt, 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



Gewusst wie?

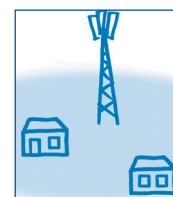


Handyortung über Funkzellen

Viele **einzelne Mobilfunkstationen**, die mit jeweils einer Mobilfunkantenne ausgestattet sind, stellen sicher, dass du mit deinem Handy überall erreichbar bist. Denn mit Hilfe von **Funkwellen** nimmt dein Handy mit der nächstgelegenen Mobilfunkantenne immer wieder kurz Kontakt auf. Es gibt sozusagen Bescheid, dass es sich noch in ihrer Reichweite befindet. Und das auch dann, wenn du nicht telefonierst oder Nachrichten verschickst.

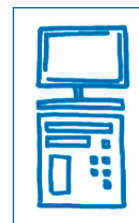


So weiß jede Mobilfunkstation, welche Handys in ihrem Versorgungsbereich eingeschaltet sind. Dieser Bereich, den eine einzelne Mobilfunkstation mit Empfang versorgt, wird auch **Funkzelle** genannt.



Über Richtfunk oder Kabel stehen die einzelnen Mobilfunkstationen mit einer zentralen **Funkvermittlungsstation** in Verbindung. Dieser zentrale Vermittlungscomputer kennt die Standorte aller eingeschalteten Mobiltelefone und leitet Daten von einer Funkzelle an eine andere Funkzelle oder auch ein anderes Telefonnetz weiter.

So kann dein Handy bzw. die Funkzelle, in der sich dein Handy befindet, innerhalb weniger Sekunden gefunden werden.



Funkzellen sind unterschiedlich groß. Im städtischen Gebiet mit vielen MobilfunkteilnehmerInnen und einem hohen Bebauungsgrad gibt es viele kleine Funkzellen. Das garantiert eine gute Netzqualität, und Mobilfunkstation und Handy können mit möglichst geringer Sendeleistung arbeiten. Im ländlichen Gebiet mit wenigen MobilfunkteilnehmerInnen und vielen unbebauten Flächen gibt es größere Funkzellen.



Wirkt sich die Größe einer Funkzelle auf das Ergebnis der Handyortung aus? Begründe deine Entscheidung!

.....

.....

.....

.....

.....

Rechenübungen zur Größe von Funkzellen

Jeder Punkt auf der Karte steht für eine Mobilfunkstation, die den Mittelpunkt einer Funkzelle darstellt.

Berechne für jede Karte, ● wie viele m^2 bzw. km^2 Fläche der jeweilige Kartenausschnitt zeigt.

- wie viele m^2 bzw. km^2 Fläche eine durchschnittliche Funkzelle in diesem Kartenausschnitt umfasst.

Karte 1 (○ = Sendemast, Maßstab 1:10.000)

Der Kartenausschnitt zeigt m^2 Fläche,

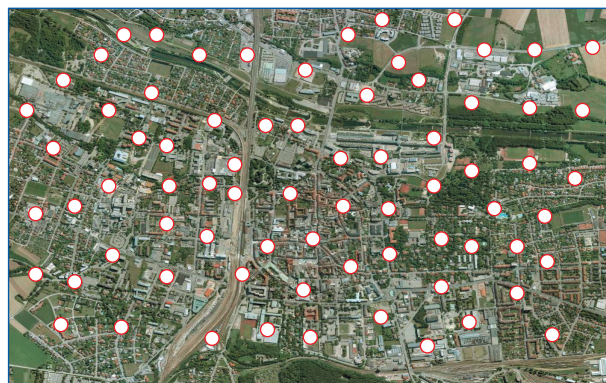
das entspricht km^2 .

Im auf der Karte angeführten Gebiet gibt es Mobilfunkstationen.

Eine Funkzelle hat durchschnittlich m^2 Fläche,

das entspricht km^2 .

Die Karte zeigt ☐ wenig besiedeltes, ländliches ☐ städtisches ☐ dicht besiedeltes, großstädtisches Gebiet.



Karte 2 (○ = Sendemast, Maßstab 1:65.000)

Der Kartenausschnitt zeigt m^2 Fläche,

das entspricht km^2 .

Im auf der Karte angeführten Gebiet gibt es Mobilfunkstationen.

Eine Funkzelle hat durchschnittlich m^2 Fläche,

das entspricht km^2 .

Die Karte zeigt ☐ wenig besiedeltes, ländliches ☐ städtisches ☐ dicht besiedeltes, großstädtisches Gebiet.



Karte 3 (○ = Sendemast, Maßstab 1:240.000)

Der Kartenausschnitt zeigt m^2 Fläche,

das entspricht km^2 .

Im auf der Karte angeführten Gebiet gibt es Mobilfunkstationen.

Eine Funkzelle hat durchschnittlich m^2 Fläche,

das entspricht km^2 .

Die Karte zeigt ☐ wenig besiedeltes, ländliches ☐ städtisches ☐ dicht besiedeltes, großstädtisches Gebiet.



Handyortung via Satellit

Ein Satellitensystem besteht aus

- Satelliten, die die Erde umkreisen und elektromagnetische Signale in Lichtgeschwindigkeit aussenden.
- Empfangsstationen auf der Erde, die diese Signale empfangen und auswerten.

Die Satellitensysteme können unterschiedliche Aufgaben erfüllen. So gibt es zum Beispiel Wettersatelliten, die die Erde beobachten und Daten sammeln, die für Wettervorhersagen genutzt werden können; Fernsehsatelliten übertragen Fernsehprogramme.

Jedes Satellitensystem sendet auf unterschiedlichen Funkfrequenzen.

Wie wird navigiert?

Jeder Navigationssatellit sendet laufend seine Koordinaten zur Erde: seine Bezeichnung, seine Position und die Sendezeit des Signals.

Der Empfänger dieses Signals kann aus der Übertragungsdauer des Signals, der so genannten Signallaufzeit, seine eigene Entfernung zum Satelliten errechnen.

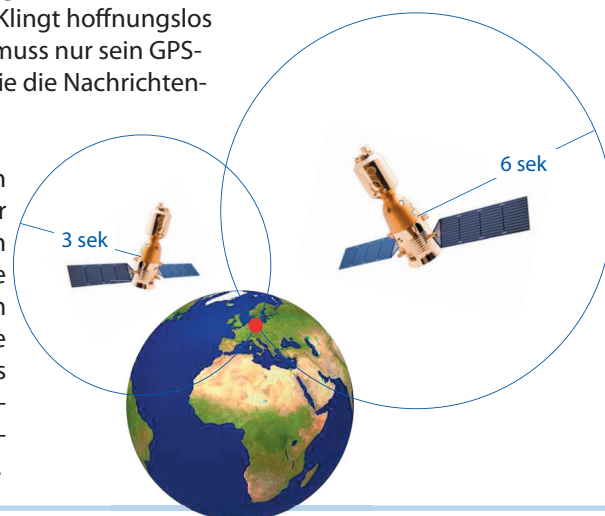
Erhält der Empfänger Signale mehrerer Navigationssatelliten, so kann er nicht nur seine Entfernung zu diesen Satelliten, sondern auch seine Position auf der Erde bestimmen.

Ein Beispiel:



Max weiß nicht weiter: Er hat sich verlaufen, und weit und breit gibt es niemanden, den er fragen könnte, wo es ihn eigentlich hinverschlagen hat. Klingt hoffnungslos – dank Hilfe aus dem All ist die Lösung allerdings einfach. Max muss nur sein GPS-Handy einschalten. Dieses sendet auf derselben Frequenz wie die Nachrichtensatelliten und empfängt daher automatisch deren Signale.

Nach kurzer Zeit trudeln auch schon Nachrichten von zwei Navigationssatelliten ein: Eine vom Satelliten Flott, der 6 Sekunden von Max entfernt ist, und die zweite vom Satelliten Flink in 3 Sekunden Entfernung. Nachdem Flott und Flink ihre genaue Position selbst bekannt gegeben haben, und nachdem dank der Signallaufzeit auch klar ist, in welcher Entfernung sie sich von Max befinden, ist die Bestimmung seines Standortes einfach: Denkt man sich um jeden der Satelliten einen Kreis, dessen Radius jeweils der Entfernung des Satelliten von Max entspricht, so befindet sich Max am Erd-Schnittpunkt dieser Kreise.



Welche Vorteile hat die Handyortung via Satellit gegenüber jener via Funkzelle?

.....

.....

Was denkst du: Kann das Handy von Max dessen Standort auch ohne Mobilfunkempfang an Dritte übermitteln?

.....

.....

7 Fliegen mit 1 Klappe

Lost and found



Navigation



Notfälle



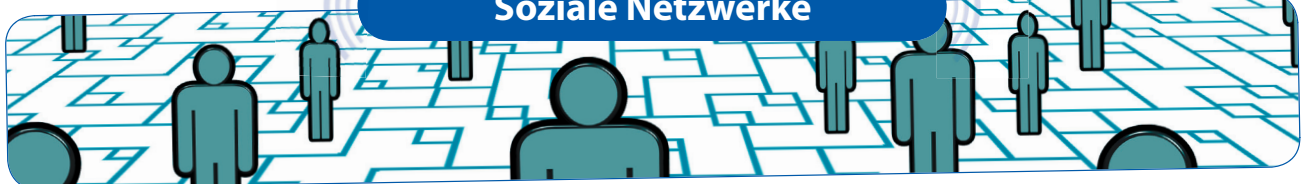
Schutzfunktionen



Sightseeing & Shopping



Soziale Netzwerke



Verbrechensverfolgung



Es war einmal ...



Geschichte 1: Nobody's perfect!

Der Plot: Lukas und Matthias werden wegen Aktivierung der Handyortungsfunktion von ihren Eltern beim Schulschwänzen erwischt.

Die Zwillinge Lukas und Matthias sind echte Sportcracks. Egal ob Sommer oder Winter – die beiden sind einfach nicht zu halten.

Das Snowboarden liegt ihnen besonders. Letzte Weihnachten haben sie von ihren Eltern sogar Smartphones mit installiertem Sicherheitsprogramm geschenkt bekommen. Mit diesem Sicherheitsprogramm können sie jederzeit geortet werden. So konnten die beiden in den Weihnachts- und Semesterferien alleine die Pisten unsicher machen und waren doch für den Notfall gerüstet.

Momentan steht den beiden allerdings der Sinn nicht nach Notfall - viel eher nach Ausfall, Stundenausfall nämlich. Der Winter ist endlich vorbei, und Lukas und Matthias freuen sich über die ersten richtig warmen Frühlingstage des Jahres. Viel zu warm, um sie in der Schule zu versetzen ...

Wie könnte diese Geschichte weitergehen?



Geschichte 2: Einbruch leicht gemacht

Der Plot: Während Elias mit seiner Familie auf Urlaub ist, wird in deren Wohnung eingebrochen. Schlussendlich stellt sich heraus, dass die Einbrecher von Elias' Social Network Profil gewusst haben, dass die Familie auf Urlaub und die Wohnung damit unbeaufsichtigt war.

Elias ist begeisterter Facebooker und Twitter. Ständig stellt er mit seinem Smartphone neue Fotos online und informiert seine vielen Freunde, von denen er nur wenige persönlich kennt, über alles, was sie schon immer von ihm wissen wollten.

Die vielen Möglichkeiten die Facebook & Twitter ihm dabei bieten, nutzt er alle aus – auch Facebook-Places: Immer wenn er sein Profil ändert, scheint daneben auf, wo er sich gerade befindet.

Natürlich darf sein cooles neues Smartphone auch im Familienurlaub nicht zu Hause bleiben. Bis ins Detail wird dokumentiert und informiert, was sich bei Familie Wallner im fernen Süden so alles tut ...

Wie könnte diese Geschichte weitergehen?

Alles sicher?

Dieser Text handelt von Sicherheitsrisiken, die bei der allzu sorglosen Nutzung von Mobiltelefonen lauern können. Ärgerlicherweise hat sich offensichtlich ein Virus eingeschlichen und sein Unwesen getrieben. Kannst du den Beschreibungen der Risiken die richtigen Bezeichnungen zuordnen?



Apps

Schadsoftware

Bluetooth- und Infrarotschnittstellen

W-LAN-Netze

Dank der Weiterentwicklung der Mobiltelefone ist unser Leben um vieles leichter und amüsanter geworden. Mit einem Handy können wir heute noch viel mehr als nur telefonieren!

Dieses Mehr an Nutzungsmöglichkeiten hat leider auch zu einem Mehr an Sicherheitsrisiken geführt. Wer diese allerdings kennt und weiß, wie er sich und seine Daten vor Missbrauch schützen kann, kann die Funktionalitäten moderner Mobiltelefone in vollem Umfang für sich nutzen.

Eine mögliche Sicherheitslücke sind

Sie ermöglichen nicht nur den einfachen Austausch von Daten, sondern sind auch eine Eingangstür zu deinem Handy. Achtest du nicht darauf, diese Tür auch wieder zu schließen, nachdem deine erwarteten Gäste eingetrudelt sind, kann es dir schnell passieren, dass plötzlich unerwünschte Eindringlinge mitten in deiner Wohnung stehen – also einfach auf dein Handy zugreifen. Und das ohne dass du es gleich bemerkst. Offene Türen knarren bekanntermaßen nicht ...

Aber auch freie können gefährlich sein. Du kannst

mit ihrer Hilfe zwar kostenlos surfen, findige Kriminelle, die technisch ein bisschen versiert sind, können dadurch allerdings auch alles mitverfolgen, was du im Internet so „treibst“. Daher solltest du, wenn du diese kostenlose Möglichkeit nutzt, um ins Internet einzusteigen, mit Passwörtern, Onlineeinkäufen oder Bankgeschäften lieber doppelt vorsichtig sein. Sonst kann dich das kostenlose Web teuer zu stehen kommen.

Smartphones sind auf dem Vormarsch. Immer mehr Kunden entscheiden sich für eines der neuen klugen Handys, die in vielen Bereichen schon den PC oder Laptop ersetzen. Damit wird diese „Zielgruppe“ auch für Programmierer interessant, die sich der Produktion von so genannter..... verschrieben haben.

Es gibt zwar noch relativ wenig bekannte Viren, Würmer und Trojaner, die Handys angreifen, aber Experten rechnen damit, dass diese Zahl in den nächsten Jahren deutlich steigen wird. Ganz nach dem Motto: „Je größer der Markt, umso vielfältiger das Angebot!“

Zu guter Letzt muss man auch die viel gerühmten und beliebten als Sicherheitsrisiko bedenken. Du hast Zeit für ein kurzes Spiel zwischendurch, suchst die nächste Öffi-Haltestelle, oder brauchst kurz einmal eine Wasserwaage? Alles kein Problem! Diese kleinen Programme bieten heute beinahe für jede Frage eine mobile Lösung. Wer allerdings bei der Installation der Miniprogramme allzu sorglos vorgeht, dem kann es passieren, dass er sich damit einen Spion ins Handy setzt. Denn manche Programme greifen auf Bereiche des Telefons zu, in denen sie eigentlich nichts verloren haben, und übermitteln Daten an den Programmhersteller, die privat sind und auch privat bleiben sollten.

Alles sicher?

Dieser Text handelt von Sicherheitsrisiken, die bei der allzu sorglosen Nutzung von Mobiltelefonen lauern können. Ärgerlicherweise haben sich offensichtlich einige Viren eingeschlichen und ihr Unwesen getrieben. Kannst du den Beschreibungen der Risiken die richtigen Bezeichnungen zuordnen? Außerdem gilt es, die richtige s-Schreibung zu ergänzen!



Apps

Schadsoftware

Bluetooth- und Infrarotschnittstellen

W-LAN-Netze

Dank der Weiterentwicklung der Mobiltelefone ist unser Leben um vieles leichter und amü anter ge-
worden. Mit einem Handy können wir heute noch viel mehr als nur telefonieren!

Dieses Mehr an Nutzungsmöglichkeiten hat leider auch zu einem Mehr an Sicherheitsri iken geführt.

Wer diese allerdings kennt und wei, wie er sich und seine Daten vor Mi brauch schützen
kann, kann die Funktionalitäten moderner Mobiltelefone in vollem Umfang für sich nutzen.

Eine mögliche Sicherheitslücke sind

Sie ermöglichen nicht nur den einfachen Austausch von Daten, sondern sind auch eine Eingangstür zu deinem Handy. Achtest du nicht darauf, die e Tür auch wieder zu schlie en, nachdem deine erwarteten Gäste eingetrudelt sind, kann es dir schnell pa ieren, da plötzlich unerwünschte Eindringlinge mitten in deiner Wohnung stehen – also einfach auf dein Handy zugreifen. Und da ohne da du es gleich bemerkst. Offene Türen knarren bekannterma en nicht ...

Aber auch freie können gefährlich sein. Du kannst mit ihrer Hilfe zwar kostenlos surfen, findige Kriminelle, die technisch ein bi chen ver iert sind, können dadurch allerdings auch alles mitverfolgen, was du im Internet so „treibst“. Daher solltest du, wenn du diese ko tenlose Möglichkeit nutzt, um ins Internet einzusteigen, mit Pa wörtern, Onlineein-
käufen oder Bankgeschäften lieber doppelt vorsichtig sein. Son t kann dich das ko tenlose Web teuer zu stehen kommen.

Smartphones sind auf dem Vormarsch. Immer mehr Kunden entscheiden sich für eines der neuen klugen Handys, die in vielen Bereichen schon den PC oder Laptop ersetzen. Damit wird diese „Zielgruppe“ auch für Programmierer interessant, die sich der Produktion von so genannter verschrieben haben.

Es gibt zwar noch relativ wenig bekannte Viren, Würmer und Trojaner, die Handys angreifen, aber Experten rechnen damit, dass diese Zahl in den nächsten Jahren deutlich steigen wird. Ganz nach dem Motto: „Je größer der Markt, um o vielfältiger das Angebot!“

Zu guter Letzt muss man auch die viel gerühmten und beliebten als Sicherheitsrisiko bedenken.

Du hast Zeit für ein kurzes Spiel zwischendurch, suchst die nächste Offi-Haltestelle, brauchst kurz einmal eine Wa erwaage oder möchtest, bevor du zur Kasse gehst, noch rasch einen aktuellen Preisvergleich durchführen? Alles kein Problem! Diese kleinen Programme bieten heute beinahe für jede Frage eine mobile Lösung!

Wer allerdings bei der Installation der Miniprogramme allzu sorglos vorgeht, dem kann es passieren, dass er sich damit selbst einen Spion ins Handy setzt. Denn manche Programme greifen auf Bereiche des Telefons zu, in denen sie eigentlich nichts verloren haben, und übermitteln Daten an den Programmhersteller, die privat sind und auch privat bleiben sollten.





Verständnisfragen zum Text „Alles sicher?“

Welche Funktionen bieten moderne Handys? Wofür kann man sie nutzen?

Wofür werden Bluetooth- und Infrarotschnittstellen beim Handy genutzt?

Hast du schon einmal eine dieser Schnittstellen genutzt? Wenn ja – wofür?

Welche Möglichkeit bieten freie W-LAN-Netze?

Hast du schon einmal ein freies W-LAN-Netz genutzt?

☐

Ja

☐

Nein

Worauf sollte man bei der Nutzung freier W-LAN-Netze achten?

Welche Bedrohungen kann man unter dem Überbegriff „Schadsoftware“ zusammenfassen?

Was solltest du bei der Installation von Apps bedenken?



Alles sicher?

Dank der Weiterentwicklung der Mobiltelefone ist unser Leben um vieles leichter und amüs^santer geworden. Mit einem Handy können wir heute noch viel mehr als nur telefonieren! Dieses Mehr an Nutzungsmöglichkeiten hat leider auch zu einem Mehr an Sicherheits^srisiken geführt. Wer diese allerdings kennt und weiß^ß, wie er sich und seine Daten vor Miss^sbrauch schützen kann, kann die Funktionalitäten moderner Mobiltelefone in vollem Umfang für sich nutzen.

Eine mögliche Sicherheitslücke sind **Bluetooth- und Infrarotschnittstellen**. Sie ermöglichen nicht nur den einfachen Austausch von Daten, sondern sind auch eine Eingangstür zu deinem Handy. Achtest du nicht darauf, diese Tür auch wieder zu schließ^ßen, nachdem deine erwarteten Gäste eingetrudelt sind, kann es dir schnell pass^sieren, dass plötzlich unerwünschte Eindringlinge mitten in deiner Wohnung stehen – also einfach auf dein Handy zugreifen. Und das^s ohne dass^s du es gleich bemerkst. Offene Türen knarren bekannterma^ßen nicht ...

Aber auch freie **W-LAN-Netze** können gefährlich sein. Du kannst mit ihrer Hilfe zwar kostenlos surfen, findige Kriminelle, die technisch ein biss^schen versⁱert sind, können allerdings auch alles mitverfolgen, was du im Internet so „treibst“. Daher solltest du, wenn du diese kost^senlose Möglichkeit nutzt, um ins Internet einzusteigen, mit Pass^swörtern, Onlineeinkäufen oder Bankgeschäften lieber doppelt vorsichtig sein. Sonst^s kann dich das kostenlose^s Web teuer zu stehen kommen.

Smartphones sind auf dem Vormarsch. Immer mehr Kunden entscheiden sich für eines der neuen klugen Handys, die in vielen Bereichen schon den PC oder Laptop ersetzen. Damit wird diese „Zielgruppe“ auch für Programmierer interess^sant, die sich der Produktion von so genannter **Schadsoftware** verschrieben haben. Es gibt zwar noch relativ wenig bekannte Viren, Würmer und Trojaner, die Handys angreifen, aber Experten rechnen damit, dass^s diese Zahl in den nächsten Jahren deutlich steigen wird. Ganz nach dem Motto: „Je größ^ßer der Markt, umso vielfältiger das Angebot!“

Zu guter Letzt muss^s man auch die viel gerühmten und beliebten **Apps** als Sicherheitsrisiko bedenken. Du hast^s Zeit für ein kurzes Spiel zwischendurch, suchst die nächste Öffi-Haltestelle, brauchst kurz einmal eine Wass^serwaage oder möchtest, bevor du zur Kass^se gehst, noch rasch einen aktuellen Preisvergleich durchführen? Alles kein Problem! Diese kleinen Programme bieten heute beinahe für jede Frage eine mobile Lösung. Wer allerdings bei der Inst^sallation der Miniprogramme allzu sorglos vorgeht, dem kann es pass^sieren, dass^s er sich damit selbst einen Spion ins Handy setzt. Denn manche Programme greifen auf Bereiche des Telefons zu, in denen sie eigentlich nichts verloren haben, und übermitteln Daten an den Programmhersteller, die privat sind und auch privat bleiben sollten.



Schutzschild aktiv?

Öffentliches WLAN ist Sicherheitsrisiko

Wer mit seinen persönlichen Daten sorglos umgeht, spielt Cyberkriminellen direkt in die Hände. Die wichtigsten Hinweise für die sichere Nutzung öffentlicher Netze.

Mobil ins Internet: Dank öffentlich zugänglichem WLAN ist das besonders einfach möglich. Doch das lockt Kriminelle an.

Mit dem Handy, dem Laptop oder dem Tablet kann heute überall ins Internet eingestiegen werden. Dabei ist öffentlich zugängliches WLAN (ein lokales Funknetz) für diesen Zugang ins Web bei den Nutzern mobiler Geräte äußerst beliebt - schließlich punktet WLAN gegenüber Mobilfunkverbindungen in der Regel mit stabileren Verbindungen. Doch diese Funknetze machen es Kriminellen gleichzeitig deutlich leichter, an sensible Daten wie Kreditkartendetails, E-Mail-Passwörter oder Informationen über das Online-Banking zu kommen, warnt das IT-Security-Unternehmen BullGuard.

Die wichtigsten Tipps

Eine beliebte Methode der Cyberkriminellen ist dabei das Installieren sogenannter Fake-APs (Access-Points). Fallen Anwender darauf herein, verbinden sie sich mit diesem falschen Netz, anstatt mit dem des bekannten WLAN-Providers. Kriminelle schneiden dann alle übertragenen Daten mit.

Aber auch ohne diesen Trick lassen sich alle Daten einholen, wenn sie unverschlüsselt über ein WLAN wandern. Stellt sich also die Frage, wie man als mobiler Nutzer dieses Risiko verringern kann. Die Security-Experten von Bull Guard geben dazu folgende Tipps für den Schutz gegen möglichen Datenklau:

- Möglichst wenig sensible Daten über das Netz senden, das gilt vor allem für unbekannte Netze.
- Zu empfehlen ist der Einsatz von verschlüsselten Verbindungen: E-Mail-Provider bieten in der Regel an, die Post über eine mit SSL oder TLS verschlüsselte Verbindung abzurufen. VPNs verbergen alle Daten vor neugierigen Blicken.
- Security-Software nutzen: Auch für Android, iPhone und Co. gibt es zahlreiche Schadpro-

gramme (Malware), die man sich im öffentlichen WLAN einfangen kann. Auf jedes Smartphone gehört daher wie bei Laptop und PC eine Security-Lösung mit Antivirensoftware und Firewall.

- WLAN ausschalten: Braucht man kein WLAN, ist es am besten, diese Funktion auf dem Gerät auszuschalten. Dann kann das Smartphone nicht automatisch eine WLAN-Verbindung aufbauen, wenn es in Reichweite eines Hotspots (öffentliches Netz) kommt. Die automatische WLAN-Erkennung und -Verbindung sollte daher ebenfalls ausgeschaltet werden.
- Um Anwender auf ihr eigenes Netz zu locken, wählen Kriminelle für das WLAN einen Namen, der dem des Providers sehr ähnlich ist. Anwender sollten also genau auf den Namen des Funknetzes achten, mit dem sie sich verbinden.

<http://wirtschaftsblatt.at/archiv/aktuell/1216217/print.do>

Böse Zwillinge / Evil Twins

Hot-Spots an öffentlichen Plätzen können von Hackern missbraucht werden. Und das könnte so aussehen: Ein Hacker setzt sich in ein Cafe und hat ein Laptop in seinem Rucksack. Dieser Laptop hat eine WLAN-Karte und ist als Access-Point ins Internet eingerichtet. Es kann auch sein, dass er den richtigen Hot-Spot im Cafe durch eine Attacke ausgeschaltet hat und alle Einstellungen auf seinen Laptop übertragen hat. Der Hacker hat nun einen sogenannten bösen Zwilling dabei. Wenn sich ein Besucher des Cafes ins Internet einloggen will, kann es sein, dass er beim bösen Zwilling landet. Der Hacker kann dann alles sehen, was das ahnungslose Opfer im Internet treibt: Er kann fremde E-Mails lesen, Passwörter stehlen und sogar an die wichtigen Daten von Kreditkarten kommen. So ein böser Zwilling kann also nicht nur sehr persönliche Daten ausspionieren, sondern auch richtig teuer werden.

http://www.handysektor.de/index.php/a_bis_z/page/boese-zwillinge-evil-twins



WLAN-Verbindung auf Smartphones absichern

Die Nutzung von WLAN vom Android-Smartphone aus ist nicht immer sicher. Wir zeigen, wie Sie WLAN-Verbindungen auf Smartphones absichern. Man hat herausgefunden, dass Google für die App-Authentifizierung bei den eigenen Diensten eine digitale Visitenkarte („Authentication Token“) häufig unverschlüsselt zurückgeschickt hat. Wird dieses Token von einem Hacker abgefangen, dann kann er sich bei Google etwa als Sie ausgeben und Ihre dort hinterlegten Daten abgreifen. Die Lücke ist mittlerweile natürlich gestopft, veranschaulicht aber ganz gut das neue Risikopotenzial der ultramobilen Geräte.

Android & iOS Smartphones vor der WLAN-Falle schützen

SSIDs öffentliche WLANs löschen: Wenn Sie mit Ihrem Smartphone oder Tablet in einem öffentlichen WLAN surfen, dann ist dessen SSID als bekannt in Ihrem Gerät hinterlegt. Falls Sie nun an einem anderen WLAN vorbeilaufen, das dieselbe SSID (und denselben Schlüssel oder keinen Schlüssel) verwendet, bucht sich Ihr Gerät automatisch dort ein. Das ist eine einfache Methode für Hacker, um Sie auszuspionieren. Löschen Sie deshalb öffentliche WLANs aus Ihrem Gerätespeicher, wenn Sie den Ort verlassen. Bei Android tippen Sie dazu auf „Menü ☒ Drahtlos und Netzwerk ☒ WLAN-Einstellungen“, danach auf das zu löschende Netz und in dem aufklappenden Fenster auf den Eintrag „Vergessen“. Bei iOS tippen Sie auf „Einstellungen ☒ WLAN“, dann rechts auf den Pfeil neben dem zu löschenden Netz und auf „Dieses Netzwerk ignorieren“.

VPN-App: Genau wie bei PC oder Notebook kann auch bei Smartphones oder Tablets ein VPN-Dienst genutzt werden, um sicher über eine verschlüsselte Vermittlungsstelle zu surfen. Eine kostenlose Möglichkeit für Android bietet hier auch wieder das Tor-Netzwerk. Laden Sie sich dazu zunächst die kostenlose App Orbot herunter, und installieren Sie sie. Nach dem Sie die App gestartet haben, tippen und halten Sie den großen Knopf in der Mitte, um sich mit dem Tor-Netzwerk zu verbinden. Nun benötigen Sie noch einen Browser, der sich über Orbot und das Tor-Netzwerk mit dem Internet verbindet. Laden Sie dazu den Browser Orweb und installieren und starten Sie ihn. Es öffnet sich eine Seite mit dem Text „Congratulations. Your browser is configured to use Tor“. Tippen Sie auf die Menü-Taste und „Go“, um eine Internetadresse eingeben und sie ansurfen zu können.

Auch hier besteht natürlich das klassische Tor-Problem. Die Verbindung ist zwar geschützt, aber auch langsam. Schnellere VPN-Dienste sind allerdings kostenpflichtig. Ein guter und schneller VPN-Dienst ist beispielsweise Vyprvpn. Der kostet ab 12,49 Euro/Monat und funktioniert mit Bordmitteln von Android, iPhone, iPad, Windows, Mac-OS X und Linux. Um ihn zu nutzen, klicken Sie auf der Internetseite auf „Buy Now“ und füllen das Formular samt Zahlungsdaten aus. Danach bekommen Sie ein Kennwort zugeschickt. Um den gesamten Datenverkehr über den Vyprvpn-Server zu leiten, folgen Sie der Anleitung für Ihr gewünschtes System unter goldenfrog.com/vyprvpn.

www.pcwelt.de/tipps/Jedes-WLAN-sicher-nutzen-WLAN-Verbindung-auf-Smartphones-absichern-4702884.html



Apps - Zusatzprogramme für das Smartphone

Sie sind seit geraumer Zeit in aller Munde - Apps, kleine Programme, die auf Smartphones installiert werden, um dessen Funktionen zu erweitern. Egal ob Spiele, News oder schlaue Helferprogramme für das alltägliche Leben - die Auswahl ist gigantisch. Kaum eine Aufgabe, die die kleinen Programme nicht lösen können.

Apps sind aus der alltäglichen Nutzung von Smartphones und inzwischen auch Tablet-Computern kaum noch wegzudenken. Die kleinen Programme, als bunte Fensterchen auf dem Touchscreen eines Smartphones zu erkennen, können in vielen Situationen sehr nützlich sein. Ebenso sind Apps ein netter Zeitvertreib: Zahlreiche Spaßprogramme, Gimmicks und Spiele in den stetig wachsenden App Online-Shops sorgen dafür, dass es immer etwas Neues zu entdecken gibt und keine Langeweile mehr aufkommt.

Was sind Apps?

App ist die englische Kurzform für „application“, was in diesem Zusammenhang so viel bedeutet wie Anwendungsprogramm. Spricht man mit Hinblick auf Handys und Tablets von Apps, sind mit dem Begriff kleine Programme gemeint, die direkt auf dem Mobiltelefon oder Tablet-Computer installiert werden können. Apps werden in speziellen, im Betriebssystem des Geräts integrierten Online-Shops angeboten, wie zum Beispiel dem Apple App Store, Googles Android Market oder der Blackberry Appworld.

App-Urgesteine

Was so modern und zukunftsweisend klingt, gibt es, wenn auch in wesentlich einfacherer Form, schon seit Jahren. Denn Handy-Anwendungen wie der Wecker, der Taschenrechner, die Stoppuhr oder der Kalender sind unter dem Strich nichts anderes als die heutigen Apps. Als jedoch die Programmiersprache Java so weiterentwickelt wurde, dass sie für Mobiltelefone nutzbar wurde, wuchsen auch die Möglichkeiten für Applikationen. Kleine Anwendungen und Spiele konnten über das Internet heruntergeladen und auf dem Telefon installiert werden. Die Möglichkeiten, die diese neue Technik schuf, waren enorm. Es dauerte jedoch bis zum Erscheinen des berühmten iPhones aus dem Hause Apple, welches diese Technik in ihrem vollen Umfang nutzte, bis auch andere Betriebssysteme wie Android nachzogen. So wurden Apps den Mobilfunknutzern in den letzten Jahren in Rekordzeit zu-

gänglich. Inzwischen gibt es in den entsprechenden Online-Shops über 500.000 Apps zum Download.

Was macht eine App aus?

Im Gegensatz zu normalen Programmen, die erst langwierig installiert werden müssen, ist eine App im Nu geladen und sofort betriebsbereit. Die Auswahl der Apps ist immens. Es gibt simple Werkzeuge und Hilfsprogramme, Spaßanwendungen, Spiele bis hin zu ganzen Programmpaketen mit umfangreichen Funktionen. Die neusten Nachrichten lesen, schnell einen Blick in den Busplan werfen, das Wetter für die nächsten Tage checken, mit einer Übersetzungshilfe nachschauen, was Gutschein auf Französisch heißt, sich schnell ein Taxi zum Aufenthaltsort rufen, Games zocken oder mal eben herausfinden, welches Lied da eben in dem Imbiss lief? Mit Apps ist das alles kein Problem. Ein Fingerzeig auf dem Touchscreen genügt. Auch für Unternehmen lohnt sich inzwischen der Einstieg ins App-Geschäft. Durch die kleinen Programme lassen sich Dienstleistungen via Smartphone in Anspruch nehmen. So beispielsweise die App-Version von Gelbe Seiten. Die Lufthansa-App bietet Fluginformationen für das Mobiltelefon.

Die Kosten für die kleinen Programme variieren. Es gibt Apps für weniger als einen Euro. Zudem sind komplexe Kleinprogramme für an die Tausend Euro verfügbar, so zum Beispiel eine App, durch die man auf Überwachungskamerasysteme zugreifen und diese mit dem iPhone steuern kann. Eine große Anzahl der Programme für das Smartphone sind hingegen auch kostenlos zu haben.

Die Macht des Apfels

Auch wenn die Erfolgsgeschichte der Apps mit dem Apple iPhone startete, haben sich heute auch andere Handy Betriebssysteme durchgesetzt. Android- und Windows-Smartphones erfreuen sich wachsender Beliebtheit. Die Apps im Apple App Store sind größtenteils kostenpflichtig. Das Angebot des Android Market besteht zu zwei Dritteln aus freien bzw. quelloffenen Programmen. Apple, Google und Microsoft erhalten beim Verkauf einer App 30 Prozent des Kaufpreises als Provision. Der Rest geht an die Entwickler.

Für den Apple App Store gab es in der Vergangenheit jedoch schon heftige Kritik. Der Grund dafür ist die Veröffentlichungspolitik, die Apple mit den Apps im Store betreibt. Denn das Geschäftsmodell gestattet es dem Hersteller, den Einsatz freier Software auf seinen Geräten zu kontrollieren. In der Praxis bedeutet dies,



dass rigoros aussortiert wird, was den Verantwortlichen nicht passt. Dieses Auswahlverfahren unterliegt Kriterien, die nicht offengelegt werden und manchmal als willkürlich erscheinen. So kann es passieren, dass Apps es niemals in den Store schaffen, oder aber im Nachhinein einfach wieder entfernt werden. Apple kann ebenso per Fernzugriff Programme auf dem iPhone löschen, die bereits im App Store gekauft wurden.

Mehr Auswahl - mehr Risiko

Im Gegensatz dazu werden Apps von Drittanbietern für das Open Source basierte Android-Betriebssystem im Adroid-Market nicht überprüft. Erst wenn ein User eine App meldet, wird diese geprüft und unter Umständen aus dem Shop entfernt. Auf diese Weise herrscht natürlich große Vielfalt im Adroid-Market. Andererseits besteht so immer die Gefahr, sich schädliche Software herunterzuladen. Derartiger Missbrauch wird durch Apple von Vornherein durch die strikten Kontrollen verhindert.

Doch es gibt weitere Probleme im Adroid-Market: Kritiker dieses App-Modells beäugen nach wie vor kritisch den Datenschutz des Systemkonzepts. Die Sorge besteht darin, Google liefere Kundendaten, die das Unternehmen vermarkten, und mit deren Hilfe ganze Datenprofile der Nutzer erstellt werden können.

Apps schreiben Erfolgsgeschichte

Die kleinen Programme sind hilfreich, nützlich oder machen einfach Laune - und es ist wohl auch ihnen zu verdanken, dass von Jahr zu Jahr mehr Smartphones verkauft werden. Zweifelsohne ist die vom Apfel Imperium verfolgte Veröffentlichungspolitik kritisch zu betrachten, aber dennoch lohnt es, sich mit der neuen Technik intensiver auseinanderzusetzen. Eine Alternative ist der Adroid-Market, doch hier ist leider nicht nur die Vielfalt größer, sondern auch das Risiko, sich unerwünschte Software zu installieren, ohne sich dessen bewusst zu sein. Wie bei jedem anderen Software-Programm sollte man also vor der Installation einer App genau schauen, woher diese stammt und ob es sich dabei um eine seriöse, vertrauenswürdige Quelle handelt. Dann steht dem Smartphone-Spaß mit all seinen Facetten nichts mehr im Wege.

www.handytarife.de/index.php?aid=2356

Wie gehe ich mit Apps sicher um?

- Fragen Sie sich, welche Apps sie **wirklich brauchen** oder unbedingt ausprobieren wollen.

- Lesen Sie die Bewertungen der Apps und **installieren sie schlecht bewertete Apps besser nicht**.
- Löschen Sie Apps, die Sie nicht mehr brauchen. Diese können **im Hintergrund** auch keine **unerwünschten Daten** mehr **übertragen**.
- Installieren Sie nur **Apps aus den offiziellen App-Shops**, da diese entweder vor der Bereitstellung **überprüft** wurden oder bei größeren Beschwerden aus dem App-Store bzw. vom Handy via Fernlöschung entfernt werden.
- Kontrollieren Sie bei der Installation von Apps die **Zugriffsberechtigungen** (z.B. bei Android-Handys bevor sie auf „Installieren“ klicken) und installieren sie eine App, die offensichtlich zu viele Berechtigungen für den Funktionsumfang bietet, lieber nicht.
- Vorsicht mit Apps, die in **sehr reißerischem Stil** oder auffallend schlechtem Deutsch für etwas werben (z.b. für einen „schnellen Gewinn in nur kurzer Zeit“, u.ä.). Die Sprache ist oft das beste Warnsignal für betrügerische Apps.
- Nehmen Sie keine **Änderungen am Handybetriebssystem** - „Jailbreak“ oder „Rooten“ genannt - vor, da dies die Installation von unsicheren Apps erleichtert und auch die Updates des Handybetriebssystems beeinträchtigen kann.
- Seien Sie besonders bei **kostenlosen Apps und damit verbundenen Werbelinks** vorsichtig. Vorsicht, wenn Kinder mit dem Smartphone spielen. Sie könnten unbemerkt Werbelinks anklicken und **unbewusst Bestellungen tätigen**.
- Sichern Sie Ihr Smartphone gegen unbefugten Zugriff (PIN-Code, **Zugriffsschutz** mit Passwort oder Entsperrmuster) und verwahren Sie es sicher.
- Installieren sie einen **mobilen Virenschutz**, um schädliche Software zu erkennen und löschen zu lassen. Es gibt zahlreiche kostenlose Schutz-Apps von bekannten Anbietern – auch in den App-Shops selbst. Diese ermöglichen u.a. auch eine Ortung Ihres verlorenen Handys, bzw. das Sperren oder Löschen persönlicher Daten.

<http://handywissen.at/was-koennen-handys/#c520>



Handy-Viren: erkennen, vermeiden, sich schützen

Handyviren sind immer noch eine Art Mythos. Jeder hat von den fiesen Mobilfunk-Schädlingen gehört. Doch anders als bei Computer-Viren kennen sich die wenigsten Menschen mit ihnen aus, geschweige denn wüssten sie, was genau ein Handyvirus ist, wie man ihn bekommt oder wie man ihm zu Leibe rückt. handytarife.de bringt Licht ins Dunkel.

Bisher sind es wenige Ausnahmen unter den Handy-Usern, die mit Gewissheit von sich behaupten können, dass ihr Mobiltelefon von einem Handyvirus infiziert wurde. Die Wahrscheinlichkeit, sich einen derartigen Schädling einzufangen, ist bis dato überaus gering. Dennoch ist es sehr wahrscheinlich, dass die Zahl der sogenannten Handyviren in Zukunft stark ansteigen wird. Das leuchtet ein, wenn man bedenkt, dass Smartphones sich steigender Beliebtheit erfreuen und bereits heute ein Großteil der Mobilfunknutzer ein internetfähiges Handy benutzt. Eine solche Entwicklung macht diese Handys und ihre Eigentümer natürlich zu einer attraktiven Zielscheibe für Kriminelle. Doch wie kann man sich vor der Gefahr durch Handyviren schützen?

Virus, Dialer, Wurm oder Trojaner?

Es gibt sowohl Handy-Viren, Handy-Dialer, Handy-Würmer als auch Handy-Trojaner - alle diese Programme gelten als Malware, also schädliche Software.

Handy-Viren sind kleine Programme, die sich auf dem Mobiltelefon einnisten und dann zum Beispiel eigenständig teure Telefonverbindungen herstellen - meistens ohne dass der Handybesitzer es überhaupt bemerkt. Auch teure Premium SMS oder MMS können auf diesem Wege versendet werden. Oft verfügen diese Programme auch über eine Funktion, die es ihnen ermöglicht, sich selbsttätig, beispielsweise über automatischen Selbstversand, weiterzuverbreiten. Ebenso ist es möglich, dass das Handy durch einen Virus, genau wie ein Computer, ausspioniert wird und die kriminellen Hintermänner auf diese Art auf die Jagd nach Bankverbindungen, Passwörtern und anderen wichtigen Daten gehen. Die Handyviren, die bisher entdeckt wurden, griffen übrigens nur Smartphones an.

Wie verbreitet sich Malware?

Bluetooth, SMS und der Internet-Download sind die gängigsten Wege, sich einen Handyvirus einzufangen.

Die schädliche Software kann über alle diese Schnittstellen auf das Handy zugreifen und beliebig Verbindungen aufbauen. Dies passiert meistens, ohne dass es der Eigentümer des Mobiltelefons bemerkt - erst wenn die horrenden Rechnung ins Haus flattert, oder sich der Datenmissbrauch auf andere Weise bemerkbar macht, stellt man den Schaden fest.

In den meisten Fällen aktivieren sich die Viren jedoch nicht selbst, sondern es ist in der Tat der Handybesitzer, der sich durch den Virus, verpackt in ein Spiel, ein Bild oder eine sonstige erhaltene Datei, dazu verführen lässt, das Programm unwissentlich zu starten.

Ähnlich wie bei Computern gibt es auch bei den Betriebssystemen, die auf einem Handy installiert sind, Sicherheitslücken und Schwachstellen, die die Hersteller der Schadsoftware gekonnt ausnutzen. Hier sind jedoch vor allem Smartphones betroffen, denn die Kombination aus Mobiltelefon und PDA liefert nicht nur ein leistungsfähiges Betriebssystem, auf dem das Virus sich optimal entfalten kann, sondern bei dieser Art von Mobiltelefon ist die Wahrscheinlichkeit, an sensible Daten wie Passwörter und Kreditkartennummern zu gelangen, am größten.

Fast immer zu spät bemerkt

Da Handy-Viren bisher bei weitem nicht so erforscht sind und wesentlich seltener auftreten, als die klassischen Computerviren, gibt es leider auch wenige Kennzeichen, die eindeutig auf eine Infektion des Mobiltelefons hinweisen.

Leider stellt man erst viel zu spät fest, dass „fremde Mächte“ auf dem eigenen Handy ihr Unwesen treiben. Wenn die Handyrechnung eine große Anzahl von Anrufen oder SMS an eine unbekannte Nummer aufweist und die Kosten scheinbar grundlos in die Höhe geschossen sind, ist dies jedoch ein ziemlich sicheres Zeichen für einen Dialer- bzw. Virenbefall. Oft haben Betroffene kurze Zeit vorher neue Programme installiert oder MMS von unbekannten Absendern erhalten, geöffnet und damit die schädlichen Programme unwissentlich installiert. Häufig nutzen diese Programme Fehler oder undichte Stellen im Betriebssystem aus.

Aber es muss nicht immer erst die hohe Telefonrechnung ins Haus flattern, bevor man merkt, dass man sich einen Virus eingefangen hat. Denn der Versand



von SMS erfolgt in der Regel durch optische oder akustische Signale, wie Töne oder das Aufleuchten des Handy-Displays. Steht das Handy also nicht mehr still oder leuchtet unentwegt auf, wird man zwangsläufig stutzig.

Wie man sich vor Handy-Viren schützen kann

Schneller als man denkt kann sich in so einem Programm, einer Nachricht oder einem harmlos wirkenden Spiel für das Handy ein böses Malware Programm verstecken. Programme, Apps und Anwendungen auf dem Smartphone zu installieren, die nicht aus vertrauenswürdigen Quellen wie den Downloadshops der Handyhersteller stammen, ist immer ein Risiko. Ebenso das Öffnen von fremden Kurz- oder Bildmitteilungen.

Sicherheitslücken im Betriebssystem sind nicht selten das Schlupfloch, durch das die Malware auf das Gerät gelangt. Die Handysoftware auf dem neuesten Stand zu halten und regelmäßig alle wichtigen Updates zu installieren, minimiert also bereits das Risiko, sich Malware einzufangen.

Auch via Bluetooth können Viren, Dialer oder Würmer auf das Handy gelangen. Daher sollte die Bluetooth-Option immer ausgeschaltet sein, wenn sie gerade nicht verwendet wird. Und bitte nicht vergessen, sie nach dem Datentransfer wieder zu deaktivieren.

Wer noch mehr tun möchte, als einfach aufmerksam zu sein und Vorsicht walten zu lassen, kann mit einer Anti-Viren Software für Handys auf Nummer sicher gehen. Hersteller von Virenschutzsoftware für Mobiltelefone sind zum Beispiel F-Secure, Kaspersky oder Symantec. Dialer- oder Einwahlblocker für Handys gibt es bis dato leider noch nicht.

Und wie wird man einen Handyvirus wieder los? Neben dem Virens Scanner, der die schädliche Software in Quarantäne setzt, empfiehlt sich ein sogenannter Masterreset, der vom Handynutzer selbst durchgeführt werden kann. Dabei wird das Telefon durch eine bestimmte Tastenkombination, die beim Hersteller erfragt werden kann, wieder auf Werkseinstellung zurückgesetzt. Alle gespeicherten Dateien und Kontakte gehen in der Regel dabei verloren, und auch die Malware wird folglich entfernt. Wer also nicht wie empfohlen seine Daten vom Handy regelmäßig extern sichert, sollte dies vor dem Reset sicherheitshalber tun.

Fazit: Vorsicht ist besser als Nachsicht

Mobiltelefone und sogenannte Smartphones erfreuen sich steigender Beliebtheit. Bisher gibt es wenige bekannte Fälle, in denen Handybesitzern großer Schaden durch Handy-Malware zugefügt wurde, und auch die Anzahl der sich im Umlauf befindenden Programme ist bisher noch überschaubar. Dennoch ist zu erwarten, dass sich auf dem Gebiet der Handy-Viren in den kommenden Jahren einiges tun wird - entsprechend ist Vorsicht angesagt. Durch die vielen Schnittstellen, über die der Datentransfer von und auf Smartphones vonstatten gehen kann, entstehen auch diverse Angriffspunkte, die es als Nutzer sorgsam zu schützen gilt. Das funktioniert am besten durch Vorsicht und eine gute Portion gesundes Misstrauen, was Software und Text- sowie Bildnachrichten fremder Absender angeht. Die regelmäßige Installation der vom Hersteller bereitgestellten Software-Updates für das Betriebssystem kann kritische Sicherheitslücken schließen. Auch ein Virens Scanner, der nach demselben Prinzip wie die klassischen Virenschutzprogramme auf dem heimischen Rechner funktionieren, bietet zusätzlichen Schutz.

www.handytarife.de/index.php?aid=1929

Handy-Viren und Handy-Dialer

Handy-Viren und Handy-Dialer haben beste Chancen, die Schädlinge der Zukunft zu werden. Rund 107 Millionen Mobiltelefone sind aktuell in Deutschland angemeldet. Grund genug für Kriminelle, Handys und Smartphones verstärkt ins Visier zu nehmen. Wie Sie sich und Ihr Mobilfunkgerät schützen können, zeigen wir Ihnen in diesem Kapitel.

Handy-Viren und Handy-Dialer: Was ist das?

Unter Handy-Dialern versteht man Programme, die sich auf dem Mobiltelefon einnisten und dann hoch tarifierte Verbindungen herstellen. Dabei kann es sich um teure Telefonverbindungen handeln. Ebenso möglich ist aber auch der Versand von hoch tarifierten Premium SMS oder MMS (Multimedia-Kurznachrichten). Handy-Viren funktionieren ähnlich. Wenn Verbindungsherstellung oder SMS-Versand vom Nutzer unbemerkt und ungewollt vonstatten gehen, handelt es sich um Schadprogramme (Malware), die je nach Ausformung auch als Handytrojaner oder Handyvirus, bzw. Handylviren bezeichnet werden. Enthält das Programm eine Funktion, über die es sich selbst - etwa



über automatischen Selbstversand – weiterverbreiten kann, ist von einem Handy-Wurm die Rede. Die Grenzen zwischen den verschiedenen Formen von Handy-Schädlingen sind allerdings noch fließend.

Wie verbreiten sich Handy-Dialer und Handy-Viren?

Moderne Mobiltelefone haben viele Schnittstellen. Die Folge ist, dass Schadprogramme wie Handy-Viren und Handy-Dialer auch mehr Möglichkeiten haben, sich zu verbreiten. Als Schnittstellen für die Infektion eines Handys können Bluetooth, SMS, aber auch der Download z.B. über eine eingesetzte SIM-Card dienen. In vielen Fällen spielt auch das so genannte Social Engineering eine Rolle: Das Schadprogramm aktiviert sich also nicht selbst, sondern bringt den Handybesitzer durch Irreführung dazu, die Aktivierung vorzunehmen. Zudem haben die Betriebssysteme von Mobiltelefonen, namentlich Windows CE und Symbian, bestimmte Sicherheitslücken, welche die Verbreitung und Installation von Schadprogrammen begünstigen.

Formen von Handy-Dialern und Handy-Viren

Zumindest bis jetzt (Stand: 2011) ist die Zahl von Programmen dieser Art überschaubar, ebenso die Zahl der konkreten Schadensfälle.

Als erster Handy-Virus ging **Cabir** in die Geschichte ein. Dieser Virus verbreitete sich über Bluetooth: Sobald das Handy angeschaltet wurde, verschickte sich Cabir selbstständig an Geräte mit offener Bluetooth-Anbindung in der Nähe.

Der erste Dialer-Trojaner für Handys verbreitete sich ebenfalls im August 2004, damals auf Mobiltelefonen mit dem Symbian-Betriebssystem Series 60. Der Trojaner verschickte ohne das Wissen des Handybesitzers SMS und steigert so die Telefonrechnung kräftig. Das Schadprogramm versteckte sich dabei in einer Raubkopie des Handy-Games Mosquitos, einer Moorhuhn-Variante des deutschen Entwicklers Ojom. Dabei handelte es sich freilich noch nicht um einen bewusst entwickelten Handy-Dialer: Der teure SMS-Versand war Medienberichten nach die Folge einer fehlgeleiteten Kopierschutzfunktion.

Konkreter wurde die Gefahr schon im Frühjahr 2005 mit dem Programm **ComWarrior**. Dieser Wurm tarnte sich hinter einer MMS-Nachricht. Öffnete man den Anhang, begann ComWarrior (ComWar) mit seiner Schadfunktion – der Weiterverbreitung per Versand an alle Adressbucheinträge des infizierten Handys.

Dadurch konnten dem betroffenen Telefonbesitzer – je nach Umfang seines Handy-Adressbuchs – horrend Schäden entstehen. In einem im Januar 2006 bekannt gewordenen Fall beklagte ein Betroffener einen Schaden von 400 Euro. Auch er hatte ganz offensichtlich nicht bemerkt, dass sein Handy plötzlich und ungewollt etliche teure MMS verschickte.

Im Februar 2006 brachte dann ein Trojaner mit Namen **J2ME/RedBrowser.A** arglose Kunden der russischen Mobilfunkbetreiber MTS, Beeline und Megafon um ihr Geld. Wie der Antivirus-Hersteller Kaspersky berichtete, musste der 54482 Byte große Schädling als gewöhnliches Java-Archiv mit Namen "redbrowser.jar" auf Handys wie eine normale Applikation installiert und ausgeführt werden. Einmal gestartet gab der Handy-Dialer in einer auf Russisch verfassten Anleitung vor, WAP-Seiten per SMS ohne Datenverbindung abrufen zu können, wobei die ersten fünf Megabyte beziehungsweise 650 SMS kostenlos seien. Statt der WAP-Seiten bekam der Handybesitzer allerdings eine überhöhte Telefonrechnung präsentiert, da die gewählten netzinternen Premium-SMS-Nummern mit rund fünf US-Dollar pro Nachricht abgerechnet wurden. Deutsche Kunden waren von diesem Dialer nicht betroffen.

Im April 2006 tauchte **RommWar** erstmals auf. Der Trojaner überschrieb bei der – manuellen – Installation eine Systemdatei und sorgt dafür, dass diese beim nächsten Neustart des Handys ausgeführt wird. In der Folge sorgte RommWar dafür, dass bestimmte Gerätefunktionen ausfielen oder das Mobiltelefon überhaupt nicht mehr startete.

Ende 2009 tauchte der Trojaner **Java/Swapi.B** auf. Der Handydialer bestand Medienberichten zufolge aus einem Java-Programm, das auf den meisten Mobiltelefonen lauffähig war. In der Software waren teure Premium-SMS-Nummern hinterlegt. An diese sendete der Dialer dann heimlich und ohne Zutun des Handy-Besitzers SMS.

Botnetze durch Handy-Trojaner

Ab 2008 wurden auch Handy-Trojaner bekannt, die dazu geeignet waren, regelrechte Bot-Netze zu bilden. In diesem Fall könnten tausende und zehntausende Mobilfunkgeräte von einem Dritten, dem "Lenker" der infizierten Geräte, dazu missbraucht werden, einen Angriff auf ein Mobilfunknetz zu starten und dieses sogar lahm zu legen. Ziel der Aktion: Der Täter, der die Handys mit Trojanern infiziert hat, könnte die

Betreiber von Mobilfunknetzen erpressen nach dem Motto "Zahlt, sonst lasse ich einen Angriff auf euer Netz starten."

Welche Handys sind betroffen?

Handy-Dialer und ähnliche Schadprogramme benötigen ein leistungsfähiges Betriebssystem, um funktionieren zu können. Insofern sind alle moderneren Mobiltelefone (Smart-Phones) betroffen. Grundsätzlich gilt: Je mehr Möglichkeiten ein Handy hat, umso mehr Möglichkeiten haben auch Viren, Trojaner und Dialer, das Gerät zu infizieren und darauf aktiv zu werden.

Woran erkenne ich, dass mein Handy oder mein Smartphone infiziert ist?

Da die Zahl der Schadprogramme für Mobiltelefone bislang gering ist, lässt sich hier keine generelle Aussage treffen.

- Ein Alarmsignal ist mit Sicherheit, wenn Ihr Mobiltelefon ungewollt und ohne äußeren Einfluss plötzlich mit dem Versand von SMS, MMS oder Premium-SMS beginnt, bzw. Telefonverbindungen herstellt. Erkennbar ist dies entweder an den bekannten akustischen Signalen (Pieps-Ton) oder am plötzlichen Aufleuchten des Displays.
- Ein ganz konkretes Anzeichen für einen Dialer oder Trojaner-Befall sind natürlich unerwartete Posten auf der Mobilfunkrechnung. Tritt hier eine massive Häufung von Ihnen unbekannten Verbindungen oder Posten für den Kurznachrichten-Versand auf, sollten Sie misstrauisch werden. Das gilt vor allem dann, wenn Sie kurz zuvor neue Programme auf Ihrem Smart-Phone installiert haben oder Kurznachrichten (MMS) von Ihnen unbekannten Absender erhalten und geöffnet haben.

Schutz vor Handyviren und Handydialern

Aktuell sind keine Handyviren oder Handydialer bekannt, die sich selbst auf dem Mobilfunkgerät installieren und aktivieren. Insofern ist der beste Schutz gesundes Misstrauen und eine gewisse Vorsicht.

- Installieren Sie auf Ihrem Mobiltelefon niemals Programme, deren Herkunft und Funktionsweise Sie nicht kennen.
- Schalten Sie die Bluetooth-Verbindung an Ihrem Handy aus. Aktivieren Sie diese nur, wenn Sie sie wirklich benötigen und deaktivieren Sie sie anschließend wieder.
- Denkbar ist auch der Schutz durch spezielle Antiviren-Software für Handys. Eine Übersicht über die gängigen Programme finden Sie bei unseren Downloads. Dialer- oder Einwahlblocker für Mobiltelefone sind bislang nicht auf dem Markt.

Ausblick und Entwicklung

Die weiter zunehmende Verbreitung von mobilen Endgeräten wie Handys und die damit verbundenen neuen Möglichkeiten machen es sehr wahrscheinlich, dass auch die Zahl der auf Mobiltelefone spezialisierten Schadprogramme zunehmen wird. Damit verbunden werden sich dubiose Anbieter auch neue Formen der Abzocke überlegen. Voraussetzung für eine Verbreitung von kostspieligen Handy-Dialern wird allerdings sein, dass sich die Täter Möglichkeiten der Gewinnabschöpfung schaffen – dass sie also unmittelbar und finanziell von den Schadfunktionen profitieren können. Dies könnte sowohl bei Premium SMS, als auch bei der Telefonie über Premium-Nummern gelingen.

www.computerbetrug.de/telefonabzocke/handyviren-und-handy-dialer



Wozu dienen Bluetooth- und Infrarot-Anschlüsse?

Bluetooth ist eine Funktechnik zur drahtlosen Sprach- und Datenübertragung zwischen elektronischen Geräten im Nahbereich. Bluetooth wird zum Beispiel für kabellose Freisprecheinrichtungen genutzt oder um zwischen Handys Fotos und Videos zu tauschen.

Bluetooth soll die Infrarot-Schnittstelle ablösen. Bei einer Datenübertragung über Infrarot ist es notwendig, dass die Handys im richtigen Abstand unbewegt nebeneinander liegen und es kann auch nur eine bestimmte Datenmenge geschickt werden.

Der Bluetooth-Standard weist drei Klassen auf und kann etwa 10, 50 oder 100 Meter weit funken. Die meisten Handys haben eine Reichweite von etwa 10 Metern.

Verbindungsaufbau: Voraussetzung ist, dass Bluetooth eingeschaltet und das Gerät für Bluetooth sichtbar ist. Sobald ein Bluetooth-Gerät aktiviert ist, beginnt es nach anderen zu suchen. Wenn sich zwei Bluetooth-Handys gefunden haben, können sie untereinander Daten austauschen. Dafür müssen jedoch beide Handy-BesitzerInnen das gleiche Passwort eingeben bzw. den Datentausch akzeptieren.

Damit dann eine Datenübertragung zwischen Bluetooth-Geräten wirklich funktioniert, ist es auch erforderlich, dass sie über die gleichen „Profile“ verfügen. „Profile“ legen fest wie genau Daten für einen bestimmten Zweck übertragen werden können, z.B. für Headsets oder Audio-Übertragungen.

Mit Bluetooth können Daten bis zu einer Übertragungsrate von 700 kBits/s im Frequenzbereich von 2,4 GHz übertragen werden. In Entwicklung ist ein Standard, der bis zu 100 MBits/s übertragen kann. Bluetooth wechselt bis zu 1.600-mal in der Sekunde die Frequenz innerhalb von 79 Frequenzstufen. Das verringert Funkstörungen und erhöht die Sicherheit. Im Vergleich zur Infrarottechnik ist ein Sichtkontakt bei Bluetooth nicht unbedingt notwendig. Bluetooth-Geräte müssen während der Datenübertragung auch nicht stillgehalten werden.

<http://handywissen.at/was-koennen-handys/#c302>

Bluetooth funkt auf kurzen Wegen

Bluetooth ist eigentlich dafür entwickelt worden, dass ein Handy ohne Kabel mit einem Zusatzgerät verbunden werden kann. So gibt es heute zum Beispiel Headsets und Freisprecheinrichtungen, die mit Bluetooth funktionieren. Bei Bluetooth werden Daten per Funk übertragen. Die meisten Handys haben auch eine Infrarot-Schnittstelle. Das funktioniert über Lichtsignale. Um Daten mit Infrarot zu tauschen, müssen sich die Handys also „sehen“. Bluetooth funktioniert auch, wenn man das Handy in der Hosentasche hat. Allerdings funkt Bluetooth bei vielen Geräten nur auf eine Entfernung von etwa 10 Metern. Bluetooth gibt es nicht nur bei Handys. Auch Laptops, PCs und sogar manche Spielekonsole nutzen Bluetooth zum Austausch von Daten.

Finde ein blaues Handy in deiner Nähe!

Jedes Handy mit Bluetooth-Funktion hat einen eigenen Namen. Das ist meist ein Produktname des Herstellers. Den Namen des Handys kann man allerdings auch selbst ändern. Mit einem Bluetooth-Handy kann man andere Geräte mit Bluetooth-Funktion in einem Umkreis von mindestens 10 Metern suchen, wenn keine Wände dazwischen liegen. Im Handy gibt es dafür eine Funktion zum Suchen von anderen Bluetooth-Geräten. Ein anderes Handy kann nur dann gefunden werden, wenn dort Bluetooth eingeschaltet ist. Außerdem kann der Bluetooth-Name auf unsichtbar geschaltet werden. Dann funkt das Handy seinen Namen nicht offen in die Welt hinein und kann nicht so leicht gefunden werden.

Wenn die Handys sich paaren

Wenn sich zwei Bluetooth-Handys gefunden haben, können Sie untereinander Daten austauschen. Dafür müssen jedoch beide Handy-Besitzer das gleiche Passwort eingeben. Die Verbindung zwischen den beiden Geräten ist dann verschlüsselt. Für die sichere Bluetooth-Paarung ist es wichtig, den Anweisungen der Geräte genau zu folgen. Wenn es möglich ist, sollten die sicheren Einstellungen aktiviert werden.

Achtung: Hintertüren bei Bluetooth

Bei Bluetooth werden Daten durch die Luft gesendet und empfangen. Leider kommt es immer häufiger vor, dass Hacker sich über diesen Funkweg Zugang zu fremden Handys verschaffen. Dann können die Daten (Adressbuch, SMS, Bilder) auf dem gehackten

Handy gelesen und verändert werden (BlueSnarfing). Außerdem kann über das fremde Handy telefoniert oder eine SMS verschickt werden (BlueBugging). Der Handy-Besitzer bekommt davon meist gar nichts mit. Ein anderer Angriff auf Bluetooth-Handys ist das sogenannte BlueSmack. Dabei werden alle anfälligen Geräte, die in Reichweite sind, gestört. Grundsätzlich kann jede Funkverbindung durch einen Störsender sabotiert werden (Jamming). Die Reichweite von Bluetooth-Handys beträgt normalerweise etwa 10 Meter. Andere Bluetooth-Geräte können über 100 Meter weit funken. Bei einer öffentlichen Vorführung wurde sogar schon ein Bluetooth-Angriff aus fast 2 Kilometer Entfernung durchgeführt. Für einen Hackerangriff werden meist Laptops mit entsprechender Software und spezielle Antennen genutzt. Allerdings gibt es auch Programme, um mit Handys einen Bluetooth-Angriff zu starten.

Ich geh auf Nummer Sicher

Um sich vor Hackerangriffen zu schützen sollte der Bluetooth-Name eines Handys auf unsichtbar gestellt werden. Dann ist es schwerer, das Handy zu orten. Allerdings gab es auch Angriffe auf Handys, deren Bluetooth-Name unsichtbar war. Denn die grundlegende Bluetooth-Funktion ist dann noch immer aktiv. Sicherer ist es, Bluetooth am Handy ganz auszuschalten, wenn es nicht benutzt wird. Besonders an öffentlichen Plätzen kann es gefährlich sein, wenn Bluetooth aktiviert ist. Außerdem sollte man sich gut überlegen, mit wem man eine Bluetooth-Paarung macht. Und wenn es keine dauerhafte Verbindung zwischen zwei Geräten sein soll, sollte die Verbindung nach dem Tausch von Daten wieder gelöscht werden. Sonst kann einem leicht etwas untergeschoben werden.

www.handysektor.de/index.php/aktuelles/netzwerk_more/immer_mehr_handys_machen_blaue



Getroffen?



Text

Bewertung nach dem Schulnoten-System: 1 = sehr gut, 5 = nicht genügend.

	Apps	Bluetooth	W-LAN	Schad- programme
Der Titel ist aussagekräftig.				
Der Einstieg regt zum Weiterlesen an.				
Die Risikobeschreibung - stimmt. - ist verständlich. - eignet sich für Menschen ab 70.				
Die Sicherheitstipps sind - verständlich. - einfach umsetzbar. - für Menschen ab 70 geeignet.				

Bild

Falls grafische Elemente eingesetzt wurden, werden diese ebenfalls nach dem Schulnotensystem bewertet.

	Apps	Bluetooth	W-LAN	Schad- programme
Wie gut unterstreichen die grafischen Elemente die Aussage/n des Textes?				
Sind sie für die Zielgruppe geeignet?				

Die Zielgruppe

Ist das Infoblatt für SeniorInnen ab 70 geeignet?

	Sehr gut	Gut	Einiger- maßen	Eher nicht	Gar nicht
Apps					
Bluetooth					
W-LAN					
Schadprogramme					



Was ist bei der Zielgruppenaufbereitung besonders gelungen?

Apps	
Bluetooth	
W-LAN	
Schadprogramme	

Was sollte geändert werden, um die Zielgruppe besser zu erreichen?

Apps	
Bluetooth	
W-LAN	
Schadprogramme	

Gesamtbeurteilung

Wie gut eignet sich das Informationsblatt, um SeniorInnen ab 70 handyfit zu machen?

	Sehr gut	Gut	Einigermaßen	Eher nicht	Gar nicht
Apps					
Bluetooth					
W-LAN					
Schadprogramme					

Ist es gelungen, keine Angst zu schüren, sondern Kompetenz und Sicherheit im Umgang mit dem Mobiltelefon zu vermitteln?

	Sehr gut	Gut	Einigermaßen	Eher nicht	Gar nicht
Apps					
Bluetooth					
W-LAN					
Schadprogramme					



Ausradiert und für immer gelöscht?

Du hast zum Geburtstag ein neues Smartphone bekommen und trittst dein altes großzügigerweise an deine kleine Schwester ab. Das gilt allerdings nur für das Handy – deine Kontakte, Fotos, SMS und MMS möchtest du ihr nicht vererben.



Was tun? In welcher Reihenfolge setzt du die folgenden Schritte?



Ich entferne die SIM-Karte und zusätzliche Speicherkarten.



Falls die Rücksetzung auf die Werkseinstellungen nicht möglich ist, nutze ich eine App, um den Telefonspeicher endgültig zu löschen.



Jetzt kann sich meine kleine Schwester freuen und meinem alten Handy mit jeder Menge frischer Daten neues Leben einhauchen!



Wenn es die Möglichkeit gibt, mein Handy auf die Werkseinstellungen zurückzusetzen, wähle ich diese Methode. So kann ich sicher sein, dass meine persönlichen Daten nicht wieder hergestellt werden können.



Dann werfe ich einen Blick in die Beschreibung meines Telefons, um mich darüber zu informieren, wie ich meine persönlichen Daten endgültig löschen kann.



Dabei muss ich darauf achten, dass es drei verschiedene Speicherplätze gibt: die SIM-Karte, den Telefonspeicher und zusätzliche Speicherkarten.



Zuerst einmal sichere ich alle Daten, die ich nicht verlieren möchte.





Ausradiert und für immer gelöscht?

1

Zuerst einmal sichere ich alle Daten, die ich nicht verlieren möchte.



2

Dabei muss ich darauf achten, dass es drei verschiedene Speicherplätze gibt: die SIM-Karte, den Telefonspeicher und zusätzliche Speicherkarten.



3

Dann werfe ich einen Blick in die Beschreibung meines Telefons, um mich darüber zu informieren, wie ich meine persönlichen Daten endgültig löschen kann.



4

Wenn es die Möglichkeit gibt, mein Handy auf die Werkseinstellungen zurückzusetzen, wähle ich diese Methode. So kann ich sicher sein, dass meine persönlichen Daten nicht wieder hergestellt werden können.



5

Falls die Rücksetzung auf die Werkseinstellungen nicht möglich ist, nutze ich eine App, um den Telefonspeicher endgültig zu löschen.



6

Ich entferne die SIM-Karte und zusätzliche Speicherkarten.



7

Jetzt kann sich meine kleine Schwester freuen und meinem alten Handy mit jeder Menge frischer Daten neues Leben einhauchen!





Hilfe: Mein Handy ist weg!

Du hast schon überall danach gesucht, versucht, dich selbst anzurufen, und trotzdem bleibt es verschwunden? Damit bist du nicht allein. Jeden Tag werden in Österreich rund 80 Handys gestohlen, andere werden verlegt oder gehen einfach verloren.

Handy weg? – SIM-Karte sperren!

Egal ob es gestohlen wurde oder ob du es einfach verloren hast: Um den Schaden so gering wie möglich zu halten, solltest du so rasch wie möglich die SIM-Karte sperren lassen!

Warum ist die Sperre der SIM-Karte wichtig? Was kannst du damit verhindern?

.....

.....

.....

Alle österreichischen Mobilfunkbetreiber bieten Hotlines zum Sperren der Handys an, bei manchen kannst du die Sperre auch übers Internet durchführen.

Achtung: Nicht registrierte Wertkartenhandys können nicht gesperrt werden – Restguthaben gehen mitsamt des Handys verloren. Restguthaben auf registrierten Wertkartenhandys bleiben nach der SIM-Karten-Sperre bestehen und können auf eine neue SIM-Karte übertragen werden.

Sperrhotlines

A1:	0800 / 664 100
Bob:	0900 / 680 680
Drei:	0800 / 30 30 30
eety:	0681 / 83083
Orange:	0699 / 70 699
tele.ring:	0820 / 650 650
Tele2mobil:	0800 / 240020
T-Mobile:	0676 / 2000
yesss!:	0820 / 810 810

Stand: Mai 2013

Gestohlen? – Ab zur Diebstahlsanzeige!

Wurde dein Handy gestohlen, solltest du nach Sperre der SIM-Karte auf alle Fälle eine Diebstahlsanzeige machen.

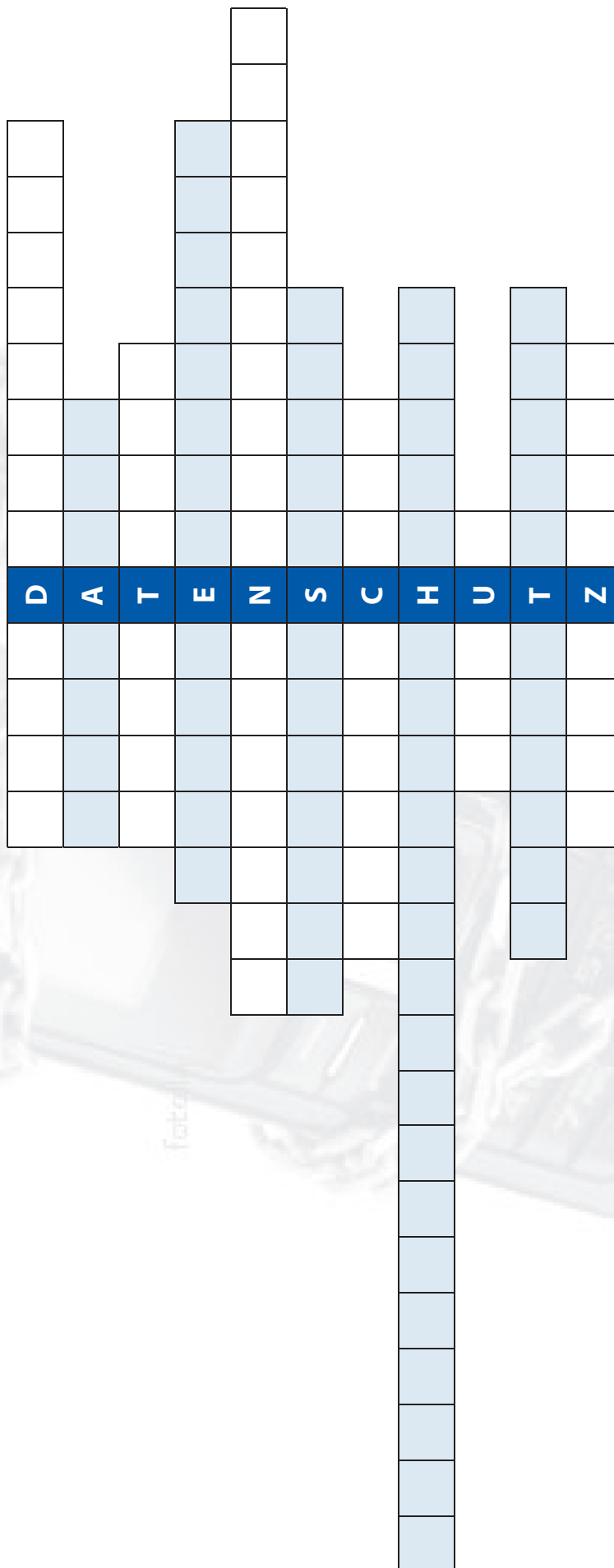
Jedes Handy hat eine **IMEI-Nummer**, das ist eine 15-stellige Seriennummer, die nur einmal vergeben wird und nicht gelöscht werden kann. Du findest sie unter dem Akku und auf der Originalverpackung deines Handys, außerdem kannst du sie mit dem Tastencode ***#06#** abfragen. Die IMEI-Nummer solltest du unbedingt notieren und im Fall eines Diebstahls der Polizei bekanntgeben. Falls dein Handy bei polizeilichen Ermittlungen gefunden oder im Fundbüro abgegeben wird, kann dank der IMEI-Nummer auch bei Löschung all deiner persönlichen Daten und Entfernung deiner alten SIM-Karte eindeutig festgestellt werden, ob es sich um dein Handy handelt.

Glück im Unglück: Mit dem Verlust eines Handys gehen nicht nur jede Menge Daten verloren – für Sperre und Neu-Ausstellung der SIM-Karte sowie den Kauf eines neuen Handys fallen auch jede Menge Kosten an. Bei Vorlage der Diebstahlsanzeige musst du bei einigen Mobilfunkbetreibern keine Gebühren für SIM-Karten-Sperre und Neuausstellung zahlen. Frag im Fall der Fälle einfach bei deinem Mobilfunkbetreiber nach.



Alles klar?

Versuche, die gesuchten Begriffe dem Rätsel zuzuordnen! Bindestriche werden diesmal ausnahmsweise ausgelassen!



- Sie versorgt dein Handy nicht nur mit Empfang, sie hilft auch, es zu orten.
- Ein Aprilscherz? Mitnichten! Hier wird nicht gescherzt, hier soll Verbrechen bekämpft werden. Deshalb ist sie seit dem 1. April 2012 in Österreich gesetzlich verankert.
- Ihr Name ist sozusagen Programm! Sie geben Auskunft darüber, wo sich ein Handy befindet.
- Diese Schnittstelle zur Datenübertragung via Funk trägt den Zahn nicht nur im Namen: In Sachen Datensicherheit zeigt sie nämlich schon mal gerne ihre Zähne und lässt allzu blauäugige SchnittstellennutzerInnen zwischendurch ganz schön blass aussehen.
- Wie sie im Detail umgesetzt wird, bleibt den einzelnen Mitgliedsstaaten überlassen. Wird sie allerdings nicht innerhalb der festgesetzten Frist in nationales Recht umgesetzt, so wie das im Fall der Vorratsdatenspeicherung in Österreich der Fall gewesen ist, so wird der säumige Staat verurteilt.
- Klingt nach aktuellem Stauservice! Tatsächlich allerdings geben sie Auskunft darüber, wann du mit wem wie lang mobil verbunden gewesen bist.
- Im Fall der Fälle schützt dich das Aus-dem-Verkehrs-Ziehen dieses kleinen Chips vor weiterem Schaden.
- Früher war dieses vor allem beim Computer Thema. Heute macht es jedes Smartphone zu einem kleinen PC. Und nachdem das tollste Handy nicht funktioniert, wenn es fehlerhaft ist, wird heute schon beim Handykauf darauf geachtet.
- Er tut weder dir noch deinem Handy gut! Beide werdet ihr davon krank.
- Mit seiner Eingabe entlockst du deinem Handy gewisse Informationen. Tippst du etwa *#06# ein, so wird die IMEI-Nummer deines Handys angezeigt, die dieses einzigartig und unverwechselbar macht.
- Ein niegel-nagel-neues Mobiltelefon verfügt über sie. Und zwar nur über sie. Werden sie wieder hergestellt, so wird alles andere gelöscht.



[illegible]

Be smart!

Die unten beschriebenen Fallbeispiele waren Teil des Einstiegs in das Thema „Datenschutz“. Jetzt, wo du mobiler Datenschutz-Profi bist, liegt es an dir: Verfasse Tipps, was man tun kann, um der jeweils beschriebenen Gefahr aus dem Weg zu gehen!



Paul S. & eine App mit unentdeckten

Als ich diese App entdeckt habe, war ich echt begeistert: „Beame mit nur einem Knopfdruck deine privaten Fotos in die Filmsets aktueller Blockbuster!“ Echt lässig! So lässig, dass sich auch alle meine Freunde über eine MMS freuen durften, in der sie an der Seite ihrer persönlichen Leinwandhelden zu bewundern waren. Echt cool! Haben übrigens auch alle meine Freunde gefunden!

Weniger cool war allerdings, dass wir kurze Zeit später mit SPAM-SMS überhäuft wurden. Und dann kam's auch schon in der Zeitung: Die Blockbuster-App konnte nämlich noch einiges mehr als auf Knopfdruck zu beamen. Ohne dass ich es bemerkt habe, hat sie auf meine persönlichen Kontakte und das Anrufverzeichnis zugegriffen. Und das Peinliche daran ist, dass ich dem App-Betreiber beim Installieren der App sogar die Erlaubnis dafür erteilt habe. Jetzt hoffe ich nur, dass nicht noch mehr Überraschungen auf mich warten. Würde mir grad noch fehlen, dass auch noch meine Handyfotos irgendwo im Web auftauchen ...



Sandra T. & verpasste Anrufe, die teuer zu stehen kommen ...

Meine letzte Handyabrechnung hat mich echt geschockt: Normalerweise zahle ich um die 12 Euro im Monat, und diesmal wurden alleine für Anrufe bei Mehrwertnummern mehr als 40 Euro verrechnet! Und das wo ich mir sicher war, keine kostenpflichtigen Nummern angerufen zu haben!

Nach dem ersten Schreck habe ich die Rechnungshotline meines Mobilfunkanbieters angerufen. Und als mich der nette Mann in der Leitung nach Anrufen unbekannter Nummern gefragt hat, war mir dann auch schon alles klar! Vor einiger Zeit hatte ich nämlich jede Menge verpasster Anrufe verschiedener Nummern. Und jedesmal wenn ich versucht habe zurückzurufen, bin ich in seltsamen Tonbandschleifen gelandet. So habe ich, ohne es zu merken, bei kostenpflichtigen Diensten angerufen und meine Telefonrechnung nach oben gekurbelt ...



Isabella F. & die teure Gratis-App

„Drohende Gefahr durch Handy-Hacker“ – bis vor kurzem hab ich mir beim Lesen solcher Schlagzeilen gedacht, dass das ja wohl maßlos übertrieben ist. Seit letzter Woche sehe ich das allerdings ganz anders! Da bin ich nämlich selbst Opfer eines heimtückischen Angriffs durch Handy-Hacker geworden. Gemeinsam mit einer Gratis-App wurde mir – ebenfalls kostenlos, allerdings auch unerwünscht – ein Trojaner mitgeliefert. Und der hat dann, ohne dass ich es bemerkt habe, SMS an alle meine Kontakte verschickt. Erst als mich eine Freundin gefragt hat, warum ich eigentlich

dauernd leere SMS versende, habe ich gecheckt, dass da etwas nicht stimmen kann und meinen Mobilfunkanbieter angerufen. Da hat sich dann herausgestellt, dass von meinem Handy täglich um die 300 SMS versendet wurden ...



Tom K. & der *unheimliche* Shoppingtrip

Eigentlich hatte ich alles perfekt geplant! Am Montagmorgen war mir einfach ganz furchtbar übel, sodass ich nicht zur Schule gehen konnte. Und nachdem meine Eltern mich gebührend bemitleidet und sich in Richtung Arbeit begeben hatten, habe ich mich dann – unentdeckt von den Nachbarn – aus dem Haus geschlichen, bin zum Bahnhof gedüst und von dort direkt nach Graz weitergefahren: Shoppen statt Schulbank drücken! Während meines kleinen Ausflugs habe ich dann auch immer wieder meinen Status auf Facebook geändert. Mit meinem neuen Smartphone geht

das ja supereasy. Da hat dann eine Statusmeldung à la „Ich fühl mich soooo schlecht“ die nächste gejagt. Grundsätzlich genial! Dumm nur, dass ich vor einiger Zeit bei Facebook die Funktion aktiviert habe, dass bei jeder neuen Statusmeldung mein Aufenthaltsort automatisch ermittelt und im Profil angegeben wird. So konnten meine Eltern auf meinem Facebook-Profil meine Shoppingtour live mitverfolgen ...



Florian E. & sein zweites Ich

Bis ich das Geld für mein neues Smartphone zusammengespart hatte, hat's eine gefühlte Ewigkeit gedauert. Die letzten Euro kamen dann noch aus der Online-versteigerung meines alten Handys. Das Glück mit meinem neuen Smartphone hat allerdings nur bis letzten Freitag angehalten. Da hat mich nämlich einer aus der Parallelklasse mächtig dumm angemacht, von wegen: „Du treibst es ja ziemlich bunt, Loverboy2000“. Erst nach langem Hin und Her ist er dann endlich damit herausgerückt, was dieser dumme Spruch sollte. Auf einem bekannten Onlinedating-Portal gab's seit neuestem ein „Loverboy2000“-Profil. Und dieses Profil war mit privaten Fotos von mir gespickt. Der Käufer meines alten Handys hatte die Bilder offensichtlich entdeckt und es für besonders witzig und originell gehalten, damit „spaßhalber“ ein Profil auf dem Onlineportal anzulegen ...



Zeynep K. & die Abofalle

Mein Klingelton hat mich schon lange genervt. Deswegen war ich auch Feuer und Flamme als ich meinen Lieblingssong als Klingelton gefunden habe. Ging auch ganz easy: Ich hab in der App einfach „Kaufen“ bestätigt, und schon stand mein neuer Klingelton zum Download bereit. So weit, so gut! Das böse Erwachen kam allerdings, als plötzlich das gesamte Guthaben auf meiner Wertkarte aufgebraucht war. Da hat sich dann herausgestellt, dass ich mit meinem Klick auf „Kaufen“ nicht nur den einen Klingelton, sondern gleich ein ganzes Klingeltonabo bestellt habe.

Ein teurer Spaß ...



Internet-Exhibitionisten „Spackeria“ „Privatsphäre ist sowas von Eighties“

Interview: Ole Reißmann; 10. März 2011.

www.spiegel.de/netzwelt/netzpolitik/0,1518,749831,00.html

Wir müssen uns von der Idee privater Daten im Internet verabschieden, sagt Julia Schramm. Im Interview mit SPIEGEL ONLINE erklärt die Mitgründerin der „datenschutzkritischen Spackeria“, warum der Datenschutz nicht mehr funktioniert und was es mit Post-Privacy auf sich hat.

SPIEGEL ONLINE: Der Datenschutz muss verbessert werden, darüber waren sich bisher Internetaktivisten und Politiker grundsätzlich einig. Alles Quatsch, sagt eine neue Gruppe, die Sie mitbegründet haben - private Daten lassen sich ohnehin nicht mehr schützen. Was will die „datenschutzkritische Spackeria“?

Schramm: Keine Macht den Datenschützern. Wir finden, dass die aktuelle Diskussion um den Schutz von Daten an der Realität vorbeigeht. Wir leben in einer vernetzten Welt, wo Privatsphäre durch das Internet nicht mehr möglich ist. Nun müssen wir sehen, wie wir damit umgehen.

SPIEGEL ONLINE: Der Grundsatz „Meine Daten gehören mir“ gilt nicht mehr?

Schramm: Das ist zwar ein schöner Anspruch, aber meine Daten können mir nicht mehr gehören. Wir haben längst die Kontrolle darüber verloren. Ob wir es nun gut finden oder nicht: Privatsphäre ist sowas von Eighties. (lacht)

SPIEGEL ONLINE: Warum holen wir uns dann nicht die Kontrolle zurück und stärken den Datenschutz?

Schramm: Wie denn? Der Aufwand, private Daten zu kontrollieren und zurückzuhalten, ist mittlerweile unverhältnismäßig hoch. Im Endeffekt können wir uns nicht dagegen wehren. Deswegen wollen wir eine Diskussion über Post-Privacy anstoßen, als Flucht nach vorne.

SPIEGEL ONLINE: Was meinen Sie mit Post-Privacy?

Schramm: Das ist erst mal eine Zustandsbeschreibung, wie der Begriff schon sagt, nach der Privatsphäre. Gleichzeitig ist es auch eine Utopie, die Idealvorstellung einer Gesellschaft, die Privatsphäre nicht mehr nötig hat, weil es keine Diskriminierung mehr gibt.

SPIEGEL ONLINE: Aber warum wird Privatsphäre dann überflüssig?

Schramm: Es mag dann zwar immer noch Platz für Privatsphäre geben, im Sinne der Trennung Hannah Arendts von öffentlichem und privatem Raum. Aber sie wird nicht mehr als Schutz notwendig. Viele Datenschützer argumentieren ja mit wirtschaftlichen und staatlichen Repressionen, die drohen, wenn die eigenen Daten nicht genug geschützt sind. Außerdem glaube ich, dass der Wunsch nach dem Schutz der Privatsphäre eine Reaktion auf eine unsichere und potentiell gefährliche Umgebung ist.

SPIEGEL ONLINE: Tatsächlich sammeln Unternehmen vielfach persönliche Daten und forschen uns aus. Das sollen wir uns gefallen lassen?

Schramm: Wir lehnen es jedenfalls ab, das mit Gewalt zu verhindern. Natürlich ist die Dominanz von einigen wenigen großen Internetfirmen wie Google oder Facebook bedenklich. Deswegen plädieren wir dafür, dass Menschen bewusst mit ihren Daten und dem Internet umgehen: Dort gibt es einfach keine Privatsphäre mehr. Aber das heißt noch lange nicht, dass Datenschutzgesetze aus der analogen Zeit das Internet einschränken müssen.

SPIEGEL ONLINE: Was ist denn das für eine Gewalt, von der sie sprechen?

Schramm: Ein Beispiel: Der Datenschützer in Niedersachsen hat dem Betreiber einer Website verboten, Google-Werbung auf seinen Seiten zu schalten. Die Begründung war, dass die IP-Adressen der Nutzer ungefragt an einen weiteren Server übertragen werden. Dabei ist das im Internet die Regel, sehr viele Seiten nutzen solche Dienste - und die Nutzer wissen das auch. Die Entscheidung dagegen ist eine Form von Staatsgewalt. [...]

SPIEGEL ONLINE: Ohne staatliche Regeln sind die Internetnutzer den Datenkraken ausgeliefert. Ist das nicht ein Widerspruch zum bewussten Umgang mit den persönlichen Daten?

Schramm: Im Internet ist es eben vorbei mit der Privatsphäre, darüber sollte man sich klar sein. Schon der Begriff Datenschutz gaukelt eine falsche Sicherheit vor, die es praktisch nicht mehr gibt. Die einzige Alternative ist, anonym zu surfen.

SPIEGEL ONLINE: Sie geben viel von sich im Internet preis, unter anderem auf Twitter und in ihrem Blog. Gibt es da Grenzen?

Schramm: Ich habe die Erfahrung gemacht, dass ich im Gegenzug auch viel zurückbekomme, neue Freundschaften, Anregungen, Unterstützung. Einige Freunde haben mir gesagt, dass ich nicht über sie schreiben soll, das respektiere ich natürlich. Und ich muss mit den Konsequenzen rechnen: Wenn ich mich irgendwo bewerbe, kann mein Chef mit Google sofort herausfinden, dass ich für die Piratenpartei bei einer Wahl angetreten bin. [...]

SPIEGEL ONLINE: Wie also soll der neue Datenschutz aussehen?

Schramm: Genau darüber wollen wir jetzt diskutieren, eine Antwort haben wir noch nicht. Nur so viel ist klar: Wir müssen den Begriff neu definieren. Was sind überhaupt schützenswerte Daten - und wie kann man sie schützen? Mit einem digitalen Radiergummi doch ganz sicher nicht.



Analysefragen

Wie definiert Schramm den Begriff „Post-Privacy“?

Schramm kritisiert Datenschützer. Welche Argumente führt sie dabei an?

Worauf führt Schramm den Wunsch vieler Menschen nach mehr Schutz der Privatsphäre zurück?

Was hältst du von Schramms Ansichten? In welchen Punkten bist du ihrer Meinung, in welchen Punkten widersprichst du ihr?



Adieu, Privatsphäre - Goodbye, verstaubter Datenschutz

Christian Heller, Vertreter der „Post Privacy“-These, erklärt, wieso Privatsphäre ausgedient hat

Interview: Eva Zelechowski, 31. Jänner 2012.

<http://derstandard.at/1325485653364/Post-Privacy-Adieu-Privatsphaere---Goodbye-verstaubter-Datenschutz>

Haben „Datenschutz“ und „Privatsphäre“ ausgedient? Während die einen auf Informationssicherheit pochen, formiert sich anderswo eine Gegenentwicklung, die sagt, dass Datenschutz nicht funktioniert - zumindest nicht in seiner bestehenden Form. Christian Heller hat als einer ihrer Vertreter das erste Buch zum Thema, „Post Privacy - Prima leben ohne Privatsphäre“, geschrieben. Darin erklärt er, wieso Datenschutz den gestellten Sicherheitsanspruch nicht erfüllt und wieso es sich ohne Privatsphäre besser lebt. [...]

derStandard.at: Sind Sie selbst bereit, komplett auf Ihre Privatsphäre zu verzichten?

Christian Heller: Ich stelle ja sehr viel von mir ins Internet, zum Beispiel über mein Wiki, wo ich meinen Tagesablauf veröffentliche. Ähnlich wie viele Nutzer von Facebook und Twitter, die dort ihr Leben „hineinverdaten“. Es ist eher ein Experiment, und ich gehe sehr vorsichtig mit der Privatsphäre anderer um. Dritte werden von mir als „X“ bezeichnet. Den Kontrollverlust möchte ich schließlich anderen nicht aufzwingen.

derStandard.at: Welche Konsequenzen haben sich aus diesem Experiment ergeben?

Heller: Außer, dass sich dadurch Scherzanrufe bei mir gehäuft haben, habe ich bisher eigentlich keine konkreten Nachteile beobachten können.

derStandard.at: Sie haben vor kurzem Ihr Buch „Post Privacy - Prima leben ohne Privatsphäre“ veröffentlicht. Welche Meinung vertreten Sie darin konkret?

Heller: Informationelle Privatsphäre, also die Kontrolle darüber, was die Welt über mein Leben wissen kann, ist immer schwerer aufrechtzuerhalten. Vor allem in Anbetracht von Digitalisierung und globaler Vernetzung. Anstatt diese Entwicklungen zu bekämpfen, sollten wir schauen, wie wir damit klarkommen und das Beste daraus machen.

derStandard.at: Wieso ist das immer schwieriger?

Heller: Wir sind umgeben von einer wachsenden Menge an Aufzeichnungsmaschinen, die Informationen sammeln, miteinander verknüpfen und auswerten. Wir selbst sind es außerdem, die immer mehr Informationen in diese Maschinerie hineinstopfen - beispielsweise die 800 Millionen User bei Facebook. Auch durch andere wird immer mehr unseres Umfelds und unserer Umrisse darin abgebildet, sodass wir gar nicht aktiv daran teilhaben müssen - irgendwann haben wir wenig Möglichkeit, unsere Privatsphäre aufrechtzuerhalten. Gleichzeitig wachsen die technologischen Möglichkeiten mit leistungsfähigeren Computern und billigeren Speichern, um aus Informationen immer mehr Wissen zu hebeln und auch mehr Informationen zu sammeln.

derStandard.at: Wir sollten also nicht versuchen uns zu wehren? Wir scheitern mit dem Versuch, unsere Privatsphäre zu wahren?

Heller: Wahrscheinlich kann man das hie und da hinausögern, indem man sich dagegen wehrt. Letztendlich denke ich, dass unsere Kraft besser investiert ist, wenn wir mit den Bedingungen aus Offenheit und Transparenz umzugehen lernen anstelle nach Mechanismen zur Geheimhaltung zu suchen.

derStandard.at: Wo sehen Sie die größten Vorteile der Post-Privacy-These? Und gilt sie für alle gleich?

Heller: Vor allem nimmt die Kommunikation und gesamt-gesellschaftliche Transparenz zu, die Gesellschaft wird dank Post-Privacy intelligenter und solidarischer. Gemeinsame Interessen oder Unterschiede werden klarer hervorgehoben, was uns auch mehr Wissen darüber verschafft, wie wir unsere Probleme angehen können. Gleichzeitig werden Machtansammlungen durchsichtiger und damit demokratisch kontrollierbarer. Hier stellt sich die Frage, ob Post Privacy für alle gleich gilt und ob sich alle allen gegenüber gleichermaßen „nackt machen“ müssen. Oder ob es Institutionen wie Geheimdienste gibt, die sich erfolgreich dagegen wehren.

derStandard.at: Wie wäre in dem Fall Ihr Lösungsansatz?



Heller: Wenn es schon einen Überwachungsapparat gibt und wenn wir unsere Privatsphäre gegenüber Körpern wie Facebook oder Geheimdiensten aufgeben müssen, muss gewährleistet sein, dass dies symmetrisch geschieht. Dann auch bitte alle Daten von allen und Bekämpfung von Informationsmonopolen, wo versucht wird, das angesammelte Wissen nur wenigen Mächtigen zur Verfügung zu stellen.

derStandard.at: Sie erwähnten vorhin eine bessere Transparenz über gemeinsame Interessen. Können Sie ein konkretes Beispiel nennen?

Heller: Ein klassisches Beispiel sind Subkulturen, die tabuisiert sind, wie zum Beispiel sexuelle Subkulturen. Die lassen sich im Internet sehr leicht finden, da sehr viele User nicht zögern, sich mit ihrem Fetisch darzustellen. Teilweise geschieht das mit Pseudonymen, es ist also nicht die totale Post Privacy, aber man findet den Mechanismus, dass man traditionelle Tabu-Themen konkret im Internet artikuliert und als Person auch ansprechbar bleibt. Das ist meines Erachtens ein ähnlicher Effekt wie in der Homosexuellen-Bewegung, die der Gesellschaft mehr Respekt eingefordert hat und sich durch die Solidarität sehr viel stärker als Gemeinschaft fühlt.

Ein anderes Beispiel sind Menschen, die aus bestimmten sozialen Bedingungen wie Hartz IV Empfänger oder - sagen wir - Freiberufler ihre Lebensumstände im Netz dokumentieren und gemeinsame Strategien im Umgang mit Behörden oder adäquate Honorar-Verrechnungen austauschen.

derStandard.at: Wir haben also Ihrer Meinung nach Vorteile durch den zunehmend wegbröckelnden Datenschutz. Finden Sie auch, dass sich für die Gesellschaft auch Nachteile durch den Datenschutz ergeben?

Heller: Zum Teil. Erstens glaube ich auch, dass Post Privacy auch Nachteile mit sich bringt, weil dadurch Sicherheiten - auf die wir angewiesen sind - infrage gestellt werden. Datenschutz hat auf jeden Fall positive Aspekte, ist aber in der jetzigen Form meines Erachtens sehr zahnlos und machtlos. Nämlich dort, wo tatsächlich Daten geschützt werden müssen. Sprich, dort wo's weh tut, ist Datenschutz nicht das große Schutzinstrument für den Einzelnen.

Andererseits ist Datenschutz deshalb erträglich, weil er so wenig fasst.

Es gibt ein erhebliches Vollzugsdefizit. Würden aber tatsächlich die deutschen Datenschutzgesetze durchgesetzt, würde man das Internet zu einem zentralistisch regulierten, stark zensierten Gebilde umwuchten müssen. Das ist aber kaum erstrebenswert. [...]

derStandard.at: Sie schreiben in Ihrem Buch, dass es eine Art Selbstkontrolle ist, seine Agenden im Netz öffentlich zugänglich zu machen. Entmündigt man sich dadurch nicht auch etwas?

Heller: Das ist ein simpler Selbstdisziplinierungstrick. Wenn man ein Mensch ist, der schwer Termine einhält, hilft es, diese anderen mitzuteilen, um den sozialen Druck zu erhöhen. Letztendlich entscheide ich aber immer noch selbst und man könnte es eher ein Selbstkontrollinstrument nennen.

derStandard.at: Bekommt die These, die Sie vertreten, viel Zustimmung?

Heller: Es sind zwar nicht alle meiner Meinung, aber grundsätzlich räumen viele ein, dass es großen Diskussionsbedarf gibt. Viele stimmen zu, dass wir mit einem bestimmten Maß an Datenschutzverlust klarkommen müssen. Selten sind meine Gesprächspartner der Ansicht, dass Datenschutz, wie er jetzt - zumindest in Deutschland - ins Gesetz gegossen ist, gut ist. Ein Großteil stimmt einer Reformierung zu. Die Dimension der Radikalität ist eher ein Streitpunkt.

derStandard.at: Es sind also immer mehr Menschen, mit denen Sie sprechen, der Meinung, dass Privatsphäre in der Form, wie sie bisher oder vor den sozialen Netzwerken bestand, ausgedient hat?

Heller: Zumindest habe ich schon lange nicht mehr mit jemandem gesprochen, der die Position „Wir müssen alles tun, um die Privatsphäre zu schützen“ vertreten hat. Da bin ich mit meinem Buch nicht alleine, es hat sich inzwischen eine Bewegung formiert. Jene, die Facebook und Co. nicht nutzen, können die Geschwindigkeit dämpfen, mit der man ins kalte Wasser der Post Privacy stürzt. Gerade Facebook und seine Gewalt ist nicht zu unterschätzen, mit der sie versuchen die Entwicklung zu ihren eigenen Gunsten voranzutreiben. Während man den Eindruck heuchelt, man würde bloß einen Trend abbilden, ist man treibende Kraft hinter der Entwicklung.

derStandard.at: Ohne Facebook gewinne ich also ein bisschen Zeit vor dem Kontrollverlust meiner persönlichen Daten?

Heller: Ja, einige Jahre bekommt man dadurch schon. Im Zweifelsfall gerät man durch die Freunde in die Maschinerie hinein. Das große Problem von Facebook ist das Ungleichgewicht der Informationen - Facebook weiß alles über uns, wir wissen nichts über Facebook. Diese Daten müssen symmetrisch sein.



Analysefragen

Welche Meinung vertritt Heller in Sachen „Post Privacy“?

Heller führt einige Vor- und Nachteile des zunehmenden Verlustes des Datenschutzes an. Wie lauten diese?

Heller spricht von mehr Transparenz in unserer Gesellschaft durch den Verlust von Datenschutz, stellt allerdings in diesem Zusammenhang auch eine konkrete Forderung. Wie lautet diese?

Wie nimmt Heller die Einstellung seiner Umwelt zu Post Privacy wahr? Welche Meinung/en sieht er hier hauptsächlich vertreten?

Welche Maßnahme/n nennt Heller, um den Verlust der Privatsphäre hinauszuzögern?

Heller kritisiert Facebook. Welche Kritikpunkte führt er an?

Was hältst du von Hellers Ansichten? In welchen Punkten bist du seiner Meinung, in welchen Punkten widersprichst du ihm?
