Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Datenschutz und Telekommunikation

Info 5

Impressum

Herausgeber:
Die Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

Postfach 14 68, 53004 Bonn
Hausanschrift: Husarenstraße 30, 53117 Bonn
Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-5550
E-Mail: referat24@bfdi.bund.de
Internet: http://www.datenschutz.bund.de

Stand: Februar 2018

Diese Broschüre ist Teil der Öffentlichkeitsarbeit der BfDI.
Sie wird kostenlos abgegeben und ist nicht für den Verkauf bestimmt.

Realisation: Appel & Klinger Druck und Medien GmbH
Bildnachweis: fotolia

Datenschutz und Telekommunikation

BfDI – Info 5

Inhaltsverzeichnis

Anhänge

Abkürzungsverzeichnis

AAV	Automatisiertes Auskunftsverfahren
Abs.	Absatz
API	Application Programming Interface
App	Applikationen
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
ca.	cirka
CAT-iq	Cordless Advanced Technology – internet and quality
CD-ROM	Compact Disc-Read Only Memory
DECT	Digital Enhanced Cordless Telecommunications
d. h.	das heißt
DIN	Deutsches Institut für Normung

DNS	Domain Name System
DoS	Denial of Service
DSL	Digital Subscriber Line
DSGVO	Datenschutz-Grundverordnung
EG	Europäische Gemeinschaft
E-Mail	Electronic Mail (Elektronische Post)
etc.	ecetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
e. V.	eingetragener Verein
EVN	Einzelverbindungsnachweis
GG	Grundgesetz
ggf.	gegebenenfalls
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
IP	Internet Protocol
https	HyperText Transfer Protocol Secure
IPv4/6	Internet Protocol Version 4/6
ISDN	Integrated Services Digital Network
IT	Informationstechnik
i. V. m.	in Verbindung mit
KDAV	Kundendatenauskunftsverordnung
KRITIS	Kritische Infrastruktur
LfD	Landesbeauftragte / Landesbeauftragter für den Datenschutz
LfDI	Landesbeauftragte / Landesbeauftragter für Datenschutz und Informationsfreiheit
LKW	Lastkraftwagen
LTE	Long Term Evolution
MMS	Multimedia Messaging Service
NotrufV	Verordnung über Notrufverbindungen
Nr.	Nummer
o. g.	oben genannt
OTT	Over-the-Top
OWiG	Gesetz über Ordnungswidrigkeiten
OVG	Oberverwaltungsgericht
PC	Personal Computer
PDF	Portable Document Format
PIN	Personal Identification Number
PUK	Personal Unblocking Key
RLTk-Bund	Richtlinie Telekommunikation Bund
s.	siehe
SIM	Subscriber Identity Module

SIP	Session Initiation Protocol
SMS	Short Message Service (Kurzmitteilung)
sog.	so genannt
s. u.	siehe unten
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikationsüberwachungsverordnung
TLS	Transport Layer Security
TMG	Telemediengesetz
TR	Technische Richtlinie
u. a.	unter anderem
UC	Unified Communications
UMTS	Universal Mobile Telecommunications System
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
USA	Vereinigte Staaten von Amerika
USB	Universal Serial Bus
usw.	und so weiter
vgl.	vergleiche
VLAN	Virtual Local Area Network
VO	Verordnung
VoIP	Voice over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
z. B.	zum Beispiel
z. T.	zum Teil

Vorwort

Wir telefonieren aus dem Festnetz, über das Internet oder per Smartphone, nutzen das Internet, kommunizieren in sozialen Netzwerken, über Messenger-Dienste und per E-Mail, versenden SMS und Telefax. Ohne Telekommunikation gäbe es kein Online-Banking, keinen E-Commerce und kein E-Government. Unser tägliches Leben ist ohne die Nutzung elektronischer Medien nicht mehr vorstellbar.

Bei all diesen Aktivitäten hinterlassen wir Datenspuren, die von Dritten erhoben, verarbeitet und verwertet werden. Vielfach sind uns nicht einmal die einschlägigen Regelungen bekannt.

Zahlreiche Gesetze und Verordnungen sollen dazu beitragen, den Datenschutz im Telekommunikationsbereich zu gewährleisten.

Diese Broschüre will interessierte Bürgerinnen und Bürger über Datenschutzfragen bei der Telekommunikation informieren. Sie soll sensibilisieren, Wissen fördern und so den Umgang mit der Technik erleichtern. Wer Technik versteht und datenschutzrechtliche Vorgaben kennt, kann Risiken besser erkennen und vermeiden. Gleichzeitig soll die Broschüre aber auch den mit diesem Thema befassten Mitarbeiterinnen und Mitarbeitern in Unternehmen und Verwaltungen ein verlässlicher Begleiter bei der täglichen Arbeit sein.

Bonn, im Februar 2018

Andrea Voßhoff
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Datenschutz und Telekommunikation

1 Überblick über die bereichsspezifischen Regelungen zum Datenschutz in der Telekommunikation

1.1 Grundgesetz

Das Fernmeldegeheimnis ist nach Artikel 10 Absatz 1 Grundgesetz (GG) unverletzlich. Dieses Grundrecht schützt den Einzelnen davor, dass der Inhalt sowie die näheren Umstände seiner Telekommunikation staatlichen Stellen zur Kenntnis gelangen. Beschränkungen dürfen nur aufgrund eines Gesetzes angeordnet werden (Artikel 10 Absatz 2 GG). Was sich hinter dem Begriff *Fernmeldegeheimnis* verbirgt, verdeutlicht § 88 Absatz 1 Telekommunikationsgesetz (TKG). Dabei bezeichnet der Begriff *Inhalt* die mittels Telekommunikationsanlagen übermittelten individuellen Nachrichten, während mit den *näheren Umständen* insbesondere die Verkehrsdaten (s. Kapitel 2.6) eines Kommunikationsvorganges gemeint sind. Artikel 10 GG regelt nur den Schutz des Fernmeldegeheimnisses im Verhältnis zwischen Bürger und Staat, besitzt aber keine unmittelbare Wirkung für den privaten Rechtsverkehr, also weder für das Verhältnis zwischen Telekommunikationsdiensteanbietern und ihren Kundinnen und Kunden noch für das Verhältnis zwischen Bürgerinnen und Bürgern untereinander.

1.2 Telekommunikationsgesetz

Das Telekommunikationsgesetz soll in erster Linie durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation fördern und so angemessene Telekommunikationsdienstleistungen gewährleisten. Im Siebten Teil des Gesetzes (§§ 88 bis 115 TKG, s. Anhang 1) befinden sich die Regelungen zum Fernmeldegeheimnis, zum Datenschutz und zur Öffentlichen Sicherheit. Die bereichsspezifischen datenschutzrechtlichen Regelungen werden in Kapitel 2 dieser Broschüre näher erörtert. Sie regeln die Rechte und Pflichten der Telekommunikationsanbieter im Umgang mit den bei der Erbringung von Telekommunikationsdiensten anfallenden personenbezogenen Daten.

Verschiedene Paragraphen des Telekommunikationsgesetzes ermächtigen die Bundesregierung, weitere Regelungen mittels Rechtsverordnung zu treffen. Oft wird die Bundesnetzagentur (BNetzA) bevollmächtigt, weitere technische Einzelheiten in einer Technischen Richtlinie (TR) festzulegen. Für den Datenschutz in der Telekommunikation sind insbesondere folgende Verordnungen relevant:

- *Telekommunikationsüberwachungsverordnung (TKÜV):* Diese Verordnung richtet sich an Telekommunikationsdiensteanbieter und legt Anforderungen an Überwachungsmaßnahmen fest. Die technischen Einzelheiten sind in der *Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR TKÜV)* dargelegt. Dort sind auch Regelungen zur Übermittlung von Anordnungen und Auskünften enthalten (s. Kapitel 2.18).

- *Verordnung über Notrufverbindungen (NotrufV)* und *Technische Richtlinie Notrufverbindungen (TR Notruf):* Hier werden die besonderen Anforderungen für Notrufverbindungen festgelegt. Aus Sicht des Datenschutzes sind die Rufnummernübermittlung und Übermittlung des Standorts relevant (s. Kapitel 2.15).

- *Kundendatenauskunftsverordnung (KDAV)* und *Technische Richtlinie Automatisiertes Auskunftsverfahren (TR-AAV):* Hier werden die Anforderungen an die automatisierte Auskunft nach § 112 TKG geregelt (s. Kapitel 2.20).

1.3 Telemediengesetz

Das Telemediengesetz (TMG, s. Anhang 2) regelt die elektronischen Informations- und Kommunikationsdienste, die im Internet angeboten werden. Hierzu gehören neben reinen Informationsdiensten (z. B. Reiseführer, Wetterdienste, Gesetzestexte und Online-Lexika) auch Suchmaschinen, soziale Netzwerke, Chatrooms und die auf Individualkommunikation angelegten Dienste, wie z. B. Online-Banking und Online-Shops. Das TMG trat 2007 an die Stelle von Teledienstegesetz, Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag und setzt in wesentlichen Teilen die E-Commerce-Richtlinie (2000/31/EG) der Europäischen Union in deutsches Recht um. Das TMG gilt gleicher-

maßen für privatwirtschaftliche und öffentliche Stellen; die einzelnen Regelungen werden in Kapitel 3.9 erläutert.

1.4 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG, s. Anhang 3) regelt den Umgang mit personenbezogenen Daten. Jegliche Verarbeitung solcher Daten (vgl. § 3 Absatz 1 BDSG) bedarf einer ausdrücklichen Erlaubnis, sei es durch ein Gesetz oder durch eine Einwilligung des Einzelnen. Das BDSG enthält Schutzregelungen für das informationelle Selbstbestimmungsrecht, etwa die Rechte der von der Datenverarbeitung betroffenen Bürgerinnen und Bürger. Das Gesetz verpflichtet die Datenverarbeiter von vorneherein, die rechtlichen Spielregeln der Datenverarbeitung zu beachten und die Bürgerinnen und Bürger über den Umgang mit ihren Daten zu informieren. Es weist den Bürgerinnen und Bürgern aber auch eine Reihe von Rechten ausdrücklich zu. Vorrangiges Ziel des Datenschutzes ist es, eine Gefährdung des Persönlichkeitsrechtes des Einzelnen durch Regeln für die Verwendung personenbezogener Daten und die Gestaltung und den Einsatz von Informationstechnik (IT) zu verhindern.

Die Entwicklung und der Einsatz datenschutzfreundlicher IT-Systeme gewinnen zunehmende Bedeutung. Im Mittelpunkt steht dabei, möglichst keine, oder – wo das nicht möglich ist – so wenig wie möglich personenbezogene Daten zu verwenden. Riesige Datenmengen sollten erst gar nicht entstehen (Grundsatz der Datenvermeidung und Datensparsamkeit gemäß § 3a BDSG). Die technisch-organisatorischen Maßnahmen, die nach § 9 BDSG zu treffen sind, sollen die Daten u. a. gegen unerlaubten Zugriff und unzulässige Verwendung sichern.

Das BDSG gilt uneingeschränkt für öffentliche Stellen des Bundes und für nicht-öffentliche Stellen (Private). Es stellt allgemeine datenschutzrechtliche Grundregeln auf, die allerdings nicht überall passen und vor allem nicht überall ausreichend sind. Darum gibt es zahlreiche datenschutzrechtliche Spezialregelungen in anderen Gesetzen wie etwa im Telekommunikationsgesetz; diese sog. *bereichsspezifischen Regelungen* gehen dem BDSG vor, d. h., sie kommen vorrangig zur Anwendung.

Ausblick: Die am 24. Mai 2016 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) gilt nach einer Übergangsfrist von zwei Jahren ab dem 25. Mai 2018 und ersetzt die bis dahin geltende EU-Datenschutzrichtlinie (Richtlinie 95/46/EG). Mit der DSGVO, die als Verordnung unmittelbar zur Anwendung kommt und keiner legislativen Umsetzung mehr bedarf, gelten zukünftig in allen Staaten der Europäischen Union grundsätzlich die gleichen Standards. Um die Regelungsspielräume der DSGVO mit Leben zu füllen, hat der Bundesgesetzgeber ein neues Bundesdatenschutzgesetz verabschiedet, dessen Regelungen das bisherige BDSG ersetzen und ganz überwiegend am 25. Mai 2018 in Kraft treten werden. Einen ersten Überblick über die neue DSGVO vermittelt die Broschüre „Datenschutz-Grundverordnung“, BfDI-Info 6. Dort und auch im Anhang 4 ist das neue BDSG enthalten.

1.5 Von der E-Privacy-Richtlinie zur E-Privacy-Verordnung

Hinter dem Begriff E-Privacy verbergen sich europarechtliche Regelungen, die ergänzend zu den allgemeinen datenschutzrechtlichen Vorschriften einen umfassenden Schutz der Privatsphäre sowie der Vertraulichkeit der Kommunikation bei der Nutzung von elektronischen Kommunikationsmitteln gewährleisten sollen. Hiermit soll vorrangig den besonderen Umständen und Herausforderungen bei der elektronischen Kommunikation als Kernelement der fortschreitenden Digitalisierung Rechnung getragen werden. Darüber hinaus dienen die Regelungen auch dazu, europaweit gleiche Wettbewerbsbedingungen für alle betroffenen Marktteilnehmende zu schaffen. Insoweit ist E-Privacy auch einer der Eckpunkte eines digitalen Binnenmarkts.

Vorschriften zu E-Privacy finden sich aktuell in der so genannten E-Privacy-Richtlinie (2002/58/EG). Diese stellt als spezialgesetzliche Regelung eine Konkretisierung und Ergänzung der allgemeinen europäischen Datenschutzrichtlinie (95/46/EG) dar. Sie wurde seit 2002 mehrfach ergänzt. Die letzte wesentliche Ergänzung erfolgte 2009 durch die Richtlinie 2009/136/EG. In Deutschland wurde die E-Privacy-Richtlinie vor allem durch Vorschriften im Telekommunikations- und Telemediengesetz, aber z. B. auch im nationalen Wettbewerbsrecht umgesetzt.

Als Ergebnis einer umfangreichen Evaluation der E-Privacy-Richtlinie hat die Europäische Kommission vorgeschlagen, diese zukünftig durch eine in allen Mitgliedsstaaten der Europäischen Union (EU) direkt anwendbare Verordnung zu ersetzen. Ziel ist es, durch eine einheitliche Rechtsanwendung in ganz Europa die EU-weite Harmonisierung des Datenschutzrechtes weiter voranzutreiben und gleichzeitig das geltende Recht besser an die Anforderungen des digitalen Zeitalters anzupassen. Die neue E-Privacy-VO soll dabei die DSGVO als Spezialgesetz konkretisieren und ergänzen.

1.6 Urheberrechtsgesetz

Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe des Urheberrechtsgesetzes (UrhG). Das Urheberrecht bezeichnet das Recht auf Schutz geistigen Eigentums in ideeller und materieller Hinsicht. Es regelt das Verhältnis des Urhebers und seiner Rechtsnachfolger zu seinem Werk und bestimmt Inhalt, Umfang, Übertragbarkeit und Folgen der Verletzung dieses Rechts.

Im digitalen Zeitalter werden Musik- oder Filmdateien oft illegal über Peer-to-Peer-Netzwerke verbreitet. Gegen diese Art der Urheberrechtsverletzung geht die Musik- und Filmindustrie als Rechteinhaber vor. Sobald eine Nutzerin oder ein Nutzer eine angebotene Datei auf den eigenen PC heruntergeladen hat, wird diese Datei häufig automatisch auf dem Computer dieses Nutzenden zum Download für andere angeboten. Das Anbieten einer urheberrechtlich geschützten Datei stellt einen Verstoß gegen das UrhG (s. Anhang 6) dar. Um solche Verstöße aufzuklären, wenden sich die Rechteinhaber vielfach an die Internet-Zugangsprovider, eine Praxis, die zahlreiche Datenschutzfragen aufwirft (s. Kapitel 3.7).

1.7 Strafprozessordnung

Jeder Diensteanbieter ist zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ausnahmen von diesem Grundsatz sind nur dann zulässig, wenn sie gesetzlich angeordnet sind. So finden sich in der Strafprozessordnung (StPO) Rechtsgrundlagen für Strafverfolgungsbehörden, aufgrund derer die Telekommunikationsunternehmen

die Überwachung der Telekommunikation zu ermöglichen haben (§§ 100a und 100b StPO) oder Auskünfte z. B. über die Bestandsdaten (§ 100j StPO) und die Verkehrsdaten (§ 100g StPO) erteilen müssen (s. Anhang 7). Von den Regelungen der §§ 113b bis 113fTKG zur sog. Vorratsdatenspeicherung abgesehen (s. hierzu Anhang 1) enthält das Telekommunikationsgesetz für Verkehrsdaten – anders als für Bestandsdaten in § 111 TKG – selbst keine gesonderte Speichererlaubnis für Zwecke der Strafverfolgung. Für eine Auskunftserteilung auf Ersuchen von Sicherheitsbehörden mit Aufgaben im Bereich der Strafverfolgung dürfen grundsätzlich nur Daten verwendet werden, die aus betrieblichen Gründen bei den Telekommunikationsunternehmen rechtmäßig gespeichert sind (s. Kapitel 3.8).

Mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl 2017 I, S. 3202) wurde in § 100a StPO in Ergänzung zur klassischen Telekommunikationsüberwachung (TKÜ) die Quellen-TKÜ als zusätzliche Maßnahme der Echtzeitüberwachung von Telekommunikationsvorgängen eingeführt. Diese neu eingeführte Regelung führt nach Auffassung der BfDI zu erheblichen datenschutzrechtlichen Risiken und wird als verfassungsrechtlich problematisch erachtet.

2 Das Telekommunikationsgesetz

2.1 Fernmeldegeheimnis

Das in § 88 TKG geregelte Fernmeldegeheimnis überträgt den grundrechtlichen Schutz des Artikel 10 Absatz 1 GG, der die Bürgerinnen und Bürger lediglich vor Eingriffen des Staates schützt, auf das Verhältnis zwischen Privaten untereinander. Dies ist erforderlich, da Telekommunikation mittlerweile weitgehend durch private Unternehmen angeboten wird.

Schutzbereich

Der Schutzbereich des § 88 TKG entspricht dem des Artikel 10 Absatz 1 GG. Geschützt sind neben dem Inhalt der Kommunikation – und zwar unabhängig vom konkreten Kommunikationsmedium – auch deren nähere Umstände. Zu diesen näheren Umständen gehören:

- die von einem Anschluss aus gewählten Rufnummern, Kennungen und Zusatzdienste, auch wenn keine Verbindung zustande kommt,
- die Rufnummern oder Kennungen der Anschlüsse, die einen anderen Anschluss angerufen haben, auch wenn keine Verbindung zustande kommt,
- bei Leistungsmerkmalen, die den Fernmeldeverkehr um- oder weiterleiten, das Umleiten, bei virtuellen Anschlüssen die jeweils zugeordneten physikalischen Anschlüsse,
- bei Mobilanschlüssen die Funkzellen, über die die Verbindung abgewickelt wird,
- Informationen zu dem jeweils in Anspruch genommenen Telekommunikationsdienst,
- Beginn und Ende der Verbindung oder des Verbindungsversuchs,
- Dauer der Verbindung.

Zeitlich erstreckt sich der Schutzbereich des Fernmeldegeheimnisses auf den Zeitraum der Nachrichtenübermittlung. Hierunter fällt auch eine eventuell notwendige Zwischenspeicherung von Informationen bei Kommunikationsmedien wie E-Mail oder netzbasierten Anrufbeantwortern. Der Übermittlungsvorgang gilt grundsätzlich erst dann als abgeschlossen, wenn die Nachricht zur Kenntnis genommen wurde und sich im Herrschaftsbereich des Empfängers befindet.

Verpflichtete

Verpflichtete nach dem Fernmeldegeheimnis sind alle Anbieter von Telekommunikationsdiensten. Nach § 3 Nr. 6 TKG sind dies neben den klassischen Telekommunikationsunternehmen auch all diejenigen, die an der Erbringung von Telekommunikationsdiensten mitwirken. Der Schutz des Fernmeldegeheimnisses wird dadurch auch auf Personen ausgedehnt, die aufgrund ihrer Tätigkeit im Zusammenhang mit Telekommunikationsdiensteanbietern theoretisch in die Lage versetzt werden, Kenntnis über geschützte Kommunikationsvorgänge zu erhalten. Dementsprechend sind auch die Anbieter von sogenannten „Over-The-Top" Diensten (wie z. B. Messengerdiensten), deren Nutzung in vielen Bereichen klassische Telekommunikationsangebote wie z. B. die SMS nicht nur überholt, sondern fast schon verdrängt hat, als Verpflichtete i. S. d. § 88 TKG zu betrachten.

Die Verpflichteten sollten ihre Mitarbeiterinnen und Mitarbeiter, deren Aufgaben in irgendeiner Weise den Anwendungsbereich des § 88 TKG berühren, auf die hieraus entstehenden Pflichten hinweisen und idealerweise ausdrücklich auf das Fernmeldegeheimnis verpflichten. Nicht an das Fernmeldegeheimnis gebunden sind Personen und Unternehmen, die die Telekommunikationsdienste bloß nutzen, ohne selbst einen Telekommunikationsdienst anzubieten, etwa die Anbieter von Websites zur direkten Kommunikation mit eigenen Kundinnen und Kunden.

Geheimhaltungspflicht

Auch Anbieter von Telekommunikationsdiensten dürfen keine Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation erhalten, sofern dies nicht zwingend für die Erbringung des Dienstes erforderlich ist (z. B. für die Abrechnung (s. Kapitel 2.7) oder die Störungsbeseitigung (s. Kapitel 2.10)), oder eine spezielle gesetzliche Vorschrift eine Kenntnisnahme erforderlich macht (z. B. bei strafprozessualen Auskunfts-

ersuchen nach § 100g StPO [s. Kapitel 3.8]). Die in diesem Zusammenhang gewonnenen Kenntnisse über Umstände, die unter das Fernmeldegeheimnis fallen, müssen geheim gehalten werden, und zwar auch über die Zeit hinaus, in der der Verpflichtete in einer dem Fernmeldegeheimnis unterliegenden Funktion tätig ist.

Verstöße gegen das Fernmeldegeheimnis

Verstöße gegen das Fernmeldegeheimnis können eine Straftat nach § 206 Strafgesetzbuch (StGB) darstellen und mit einer Geldbuße oder Freiheitsstrafe bis zu fünf Jahren geahndet werden (s. Anhang 8). Unter Umständen können daneben noch zivilrechtliche Schadensersatz- und Unterlassungsansprüche entstehen.

2.2 Anwendungsbereich

§ 91 TKG regelt den Anwendungsbereich der datenschutzrechtlichen Vorschriften des Telekommunikationsgesetzes. Geschützt werden die personenbezogenen Daten von Teilnehmenden und Nutzenden, die im Zusammenhang mit der geschäftsmäßigen Erbringung eines Telekommunikationsdienstes von deren Anbieter verarbeitet werden.

Telekommunikationsdiensteanbieter

Anbieter von geschäftsmäßigen Telekommunikationsdiensten ist nach § 3 Nr. 6 TKG jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Als Diensteanbieter im Sinne des TKG gilt man auch, wenn das Angebot von Telekommunikationsdienstleistungen nur beiläufig erfolgt. So sind beispielsweise Betreiber von Hotels oder Cafés, die ihren Gästen einen Internetzugang anbieten, Diensteanbieter (s. Kapitel 4.4.2). Gleiches gilt für Arbeitgeber, die ihren Arbeitnehmern die private Nutzung der betrieblichen Telekommunikationsinfrastruktur erlauben (s. Kapitel 4.1.6). Auch sogenannte „Over-The-Top“ Dienste (OTT-Dienste), wie z. B. Messengerdienste, die für ihr Angebot keine eigenen Netze, sondern eine unabhängig von ihrem Dienst bestehende Internetverbindung nutzen, sind als Telekommunikationsdienste zu kategorisieren.

Dabei ist der Anwendungsbereich des TKG nicht auf Anbieter öffentlich zugänglicher Telekommunikationsdienste beschränkt und umfasst grundsätzlich auch geschlossene Benutzergruppen. Soweit im Rahmen der letzten Gesetzesnovellierung die Legaldefinitionen der Begriffe Teilnehmer und Nutzer in § 3 Nr. 14 und Nr. 20 TKG geändert wurden und seitdem lediglich auf die Inanspruchnahme von öffentlich zugänglichen Telekommunikationsdiensten eingegangen wird, stellt dies wohl ein redaktionelles Versehen dar. Nach einhelliger Meinung ist der nach der Gesetzessystematik eingeschränkte Anwendungsbereich im Wege einer Analogie entsprechend zu erweitern.

Teilnehmende und Nutzende

Da der Anwendungsbereich nach § 91 Absatz 1 Satz 1 TKG die Verarbeitung personenbezogener Daten voraussetzt, kommen zunächst einmal lediglich natürliche Personen als von der Datenverarbeitung betroffene Teilnehmende und Nutzender in Frage. Allerdings erweitert § 91 Absatz 1 Satz 2 TKG den Anwendungsbereich auch auf juristische Personen und Personenstandsgesellschaften, sofern es sich um Daten handelt, die dem Fernmeldegeheimnis (s. Kapitel 2.1) unterliegen. Deswegen gelten die §§ 93ff. TKG, die die Verarbeitung von Verkehrsdaten (s. Kapitel 2.6) regeln, auch für juristische Personen und Personenstandsgesellschaften, während Vorschriften zum Umgang mit Bestandsdaten (s. Kapitel 2.5) insoweit nur einschlägig sind, wenn Daten natürlicher Personen betroffen sind.

2.3 Informationspflichten

§ 93 Absatz 1 TKG verpflichtet Diensteanbieter, ihren Teilnehmern Informationen über datenschutzrelevante Umstände ihres Vertrages zukommen zu lassen. Neben allgemeinen Angaben über die Erhebung und Verwendung personenbezogener Daten müssen die Diensteanbieter insbesondere auf die zulässigen Wahl- und Gestaltungsmöglichkeiten der Teilnehmer hinweisen.

Allgemeine Informationen

Bereits zum Zeitpunkt des Vertragsschlusses müssen die Teilnehmerinnen und Teilnehmer allgemein darüber unterrichtet werden, welche Art von Daten zu welchen Zwecken an welchen Orten und in welchem Umfang verarbeitet werden. Ebenso soll-

ten ihnen auch Informationen zur Verfügung gestellt werden, wer bei datenschutzbezogenen Anliegen und Auskunftsersuchen der korrekte Ansprechpartner im Unternehmen ist.

Zulässige Wahl- und Gestaltungsmöglichkeiten

Darüber hinaus muss der Diensteanbieter seine Teilnehmenden ausdrücklich auf die verschiedenen gesetzlich geregelten Wahl- und Gestaltungsmöglichkeiten hinweisen, die im Zusammenhang mit einem Vertrag über Telekommunikationsdienstleistungen relevant werden können. Die wichtigsten Fälle betreffen Informationen zu:

- Einträgen in Teilnehmerverzeichnisse nach § 104 TKG (s. Kapitel 2.13),
- Einträgen bei Auskunftsdiensten nach § 105 TKG (s. Kapitel 2.14),
- der Ausgestaltung des Einzelverbindungsnachweises nach § 99 TKG (s. Kapitel 2.9),
- der Einwilligungsmöglichkeit in bzw. Widerspruchsmöglichkeit gegen die Nutzung von Bestands- und/oder Verkehrsdaten, beispielsweise zu Zwecken der Werbung für oder Vermarktung von Telekommunikationsdiensten nach §§ 95 Absatz 2 und 96 Absatz 3 TKG (s. Kapitel 2.5 und 2.6), und
- der Möglichkeit nach § 102 Absatz 1 Satz 1 TKG, eine dauerhafte Rufnummernunterdrückung einzurichten (s. Kapitel 2.12).

2.4 Elektronische Einwilligung

Die datenschutzrechtlichen Regelungen im TKG folgen dem Grundsatz, dass die Verarbeitung personenbezogener Daten immer durch eine gesetzliche Grundlage oder die Einwilligung der Betroffenen erlaubt sein muss. Eine wirksame Einwilligung bedarf nach § 4a BDSG gewisser Voraussetzungen (s. Kapitel 3.1). So muss grundsätzlich die Schriftform gewahrt sein. Um zu ermöglichen, sowohl das Internet als auch eine E-Mail für den Abschluss oder die Änderung von Verträgen mit Diensteanbietern zu verwenden, enthält § 94 TKG eine Ausnahmeregelung, die die Erteilung von Einwilligungen gegenüber einem Diensteanbieter auch in elektronischer Form zulässt. Diese Abweichung von den in § 4a BDSG festgelegten Grundsätzen ist allerdings nur möglich, wenn der Diensteanbieter Folgendes sicherstellt:

- Die Einwilligung wird bewusst und eindeutig erteilt. Dies setzt voraus, dass die Nutzenden oder Teilnehmenden hinreichend über die Voraussetzungen und Folgen der Einwilligung informiert sind und die vorgegebene Erklärung (beispielsweise der Text hinter dem Kästchen, das angeklickt werden muss) eindeutig und verständlich ist.
- Die Einwilligung wird protokolliert, so dass nachvollzogen werden kann, wann welche Erklärungen abgegeben wurden.
- Der Inhalt der Einwilligung kann jederzeit vom Erklärenden abgerufen und somit auch nach längerer Zeit nachvollzogen werden, was genau seinerzeit erklärt wurde.
- Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden; dabei dürfen an den Widerruf keine höheren formellen Anforderungen gestellt werden als an die Einwilligung.

2.5 Bestandsdaten

Daten von Kundinnen und Kunden, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, bezeichnet das Telekommunikationsgesetz als Bestandsdaten, die im Rahmen des § 95 TKG erhoben und verwendet werden dürfen.

Vertragsabschluss

Generell gilt: Der Diensteanbieter darf nur nach solchen Daten fragen, die für das Vertragsverhältnis erforderlich sind. Vor Vertragsabschluss darf nach dem Namen, dem Geburtsdatum, der Adresse und den Kontoverbindungsdaten gefragt werden. Zur Überprüfung dieser Angaben kann der Diensteanbieter eine Kopie des Personalausweises anfertigen, die von ihm aber unverzüglich nach abgeschlossener Überprüfung zu vernichten ist (§ 95 Absatz 4 TKG). Auch die Bitte um Vorlage der EC-Karte und die Überprüfung, ob die Angaben im Antrag stimmen, sind zulässig. Allerdings dürfen die EC-Karten nicht kopiert werden, da dadurch zusätzliche Daten – wie z. B. Kartennummer und Gültigkeitsdatum – erhoben werden, die im Rahmen des Vertragsabschlusses nicht angegeben werden müssen.

Bei telefonischen Vertragsabschlüssen werden die erforderlichen Daten häufig in einer Gesprächsaufzeichnung dokumentiert. Vor der Einwilligung der Kundinnen und

Kunden in diese Aufzeichnung muss der Diensteanbieter auf Zweck und Dauer des Gesprächsmitschnittes hinweisen (s. Kapitel 4.7).

Häufig wird bei Vertragsabschluss auch eine Prüfung der Kreditwürdigkeit (Bonitätsprüfung) durchgeführt; dabei werden die Daten an Auskunfteien übermittelt. Dies ist gemäß § 28 Absatz 1 Nr. 1 BDSG zulässig, wenn ein Postpaid-Vertrag abgeschlossen werden soll, der Diensteanbieter also in Vorleistung tritt und der Kunde oder die Kundin erst nach erhaltener Leistung zahlt (s. Kapitel 3.4). Der Diensteanbieter hat dann ein berechtigtes Interesse an der Anfrage bei der Auskunftei (§ 28 Absatz 1 Nr. 2 BDSG). Im Fall eines schriftlichen Vertrages muss eine entsprechende Klausel auf dem Vertragsformular deutlich lesbar (z. B. durch Fettdruck hervorgehoben) sein und vor der Unterschriftenzeile stehen. Bei Vertragsabschluss am Telefon dokumentiert der Call-Center-Mitarbeitende die Zustimmung im Rahmen der Gesprächsaufzeichnung. Eine Bonitätsprüfung findet in der Regel nicht statt und wäre auch nicht zulässig, wenn man sich für ein Prepaid-Angebot entscheidet, bei dem der Diensteanbieter nicht in Vorleistung treten muss.

Löschung der Bestandsdaten

Nach § 95 Absatz 3 Satz 1 TKG muss der Diensteanbieter die Bestandsdaten mit Ablauf des auf die Vertragsbeendigung folgenden Kalenderjahres löschen. Wer also zum 31. Januar 2016 gekündigt hat, dessen Bestandsdaten werden erst nach Ablauf des 31. Dezember 2017 gelöscht. Diese Löschungsfrist ist im Vergleich zu Fristen in anderen Verträgen sehr lang. Üblicherweise sind personenbezogene Daten, die für vertragliche Zwecke verarbeitet wurden, zu löschen, sobald sie nicht mehr benötigt werden. Bei der Beendigung und damit Abwicklung eines Vertragsverhältnisses, bei dem alle gegenseitigen Pflichten erfüllt sind, reichen dafür regelmäßig kürzere Fristen. Die verlängerte Löschungsfrist hat der Gesetzgeber den Telekommunikationsdiensteanbietern mit Blick auf die Massenvertragsverhältnisse zu deren Erleichterung eingeräumt. Eine Vielzahl von Kundendaten müssen aufgrund steuer- und handelsrechtlicher Vorschriften auch über die Jahresfrist hinaus gespeichert bleiben, was nach § 35 Absatz 3 Nr. 1 BDSG zulässig ist. Die Daten sind dann jedoch nicht länger in zugänglicher und lesbarer Form gespeichert, sondern müssen gesperrt sein, d. h., sie sind nur noch einem sehr engen Kreis von Mitarbeitenden des Diensteanbieters zugänglich.

Werbung

Ob klassische Werbepost, Anrufe und Telefaxe, SMS oder E-Mail: Der Diensteanbieter darf seine Kundinnen und Kunden in der Regel nur bewerben, wenn sie zugestimmt haben (Einwilligungslösung oder sog. Opt-in, § 95 Absatz 2 Satz 1 TKG). Diese Zustimmung, Bestandsdaten zur Werbung für eigene Angebote und zur Marktforschung benutzen zu dürfen, wird häufig bereits bei Vertragsabschluss eingeholt, kann aber jederzeit beim Diensteanbieter widerrufen werden.

Darüber hinaus ist in § 95 Absatz 2 Satz 2 TKG aber auch eine Widerspruchslösung oder ein sog. Opt-out enthalten. Danach dürfen die Rufnummer sowie die Post- und E-Mail-Adresse für die Versendung von Text- und Bildmitteilungen verwendet werden, es sei denn, die Kundin oder der Kunde hat einer solchen Verwendung widersprochen. Diese Möglichkeit gilt aber nur im Rahmen einer bestehenden Kundenbeziehung und nur für Eigenwerbung der Unternehmen. Außerdem muss die betreffende Person bei der erstmaligen Erhebung oder Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht darüber informiert werden, dass jederzeit der Nutzung der Daten für Werbezwecke widersprochen werden kann.

Außerhalb bestehender Kundenbeziehungen und für die Nutzung anderer Daten als Rufnummer und Adresse gilt generell der Grundsatz, dass eine Einwilligung der jeweiligen Kundinnen und Kunden vorliegen muss. Andernfalls ist die Nutzung der Daten für Werbezwecke nicht zulässig (s. Kapitel 3.4).

2.6 Verkehrsdaten

Verkehrsdaten sind alle Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Dies betrifft nicht nur die Daten, wer wann mit wem telefoniert hat. Auch Informationen von Anrufversuchen oder diverse technische Informationen zählen zu den Verkehrsdaten, etwa Informationen zu einem Wechsel der Funkzelle („Handover“) beim Mobiltelefon. Auch bei anderen Diensten wie z. B. dem E-Mail-Versand , entstehen Verkehrsdaten.

§ 96 TKG regelt, dass Verkehrsdaten nach Ende der Verbindung unverzüglich gelöscht werden müssen, wenn sie nicht für den Aufbau weiterer Verbindungen oder für Zwecke benötigt werden, die im TKG oder anderen Gesetzen geregelt sind. Bei diesen Zwecken handelt es sich um

- Abrechnung mit dem Teilnehmer einschließlich Erstellung des Einzelverbindungsnachweises (s. Kapitel 2.9),
- Störungsbeseitigung und Missbrauchserkennung (s. Kapitel 2.10),
- Vermarktung, bedarfsgerechte Gestaltung von TK-Diensten und Bereitstellung von Diensten mit Zusatznutzen, wenn der Teilnehmer eingewilligt hat (s. u.) und
- Abrechnung der Telekommunikationsanbieter untereinander (s. Kapitel 2.7).

Mit den *anderen Gesetzen* sind u. a. Regelungen für Sicherheitsbehörden (s. Kapitel 3.8) gemeint. Diese Regelungen erlauben eine Nutzung vorhandener Verkehrsdaten; eine Vorratsdatenspeicherung, d. h. die Verpflichtung, diese Daten für mögliche künftige Belange der Sicherheitsbehörden weiter vorzuhalten, ist nur in § 113b TKG vorgesehen. Die aktuelle sog. Vorratsdatenspeicherung wurde im Frühjahr 2015 mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten beschlossen, nachdem die erste Version der Vorratsdatenspeicherung im Jahr 2010 vom Bundesverfassungsgericht (BVerfG) für verfassungswidrig erklärt wurde. Nunmehr wurden die Speicherdauer vermindert (Standortdaten vier Wochen, andere Daten zehn Wochen), der E-Mail-Verkehr ausgenommen und die Sicherheitsanforderungen deutlich erhöht. So ist eine verschlüsselte Speicherung und ein Zugang nur im 4-Augen-Prinzip vorgesehen; Details werden in dem Anforderungskatalog nach § 113f TKG geregelt. Nach einem Urteil des Gerichtshofes der Europäischen Union (EuGH) aus Dezember 2016 und einer darauf bezugnehmenden Entscheidung des Oberverwaltungsgerichts (OVG) des Landes Nordrhein-Westfalen in einem Verfahren des einstweiligen Rechtsschutzes hat die Bundesnetzagentur auf Maßnahmen zur Durchsetzung der Speicherverpflichtung vorläufig verzichtet. Deshalb war zur Zeit der Drucklegung dieser Broschüre die Vorratsdatenspeicherung praktisch ausgesetzt.

Die in § 96 Absatz 1 Satz 3 TKG vorgeschriebene *unverzügliche* Löschung der Verkehrsdaten nach Ende der Verbindung bedeutet im juristischen Sinne, dass die Daten „ohne schuldhaftes Zögern“ zu löschen sind. Neben den Hinweisen in den entsprechenden

Abschnitten können Sie auch Informationen zu den jeweiligen Speicherzeiten im „Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten“ finden (s. www.datenschutz.bund.de).

Die Regelung zur Nutzung der Verkehrsdaten zur Vermarktung etc. in § 96 Absatz 3 TKG erlaubt den Anbietern, der jeweiligen Person individuell angepasste Vorschläge für einen Tarifwechsel zu unterbreiten. Voraussetzung ist jedoch eine informierte Einwilligung (s. Kapitel 2.4 und 3.1).

2.7 Abrechnung

In § 97 TKG ist geregelt, wie die Verkehrs- und Bestandsdaten zur Entgeltermittlung und -abrechnung verarbeitet werden dürfen. Dies betrifft zunächst die Abrechnung mit der Teilnehmerin bzw. dem Teilnehmer, also die „normale“ Telefonrechnung. Dazu hat der Anbieter nach Ende der Verbindung aus den Verkehrsdaten die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden.

Bei dieser sechs-Monatsfrist handelt es sich um eine Höchstfrist. In der Praxis dürfte eine Mindestfrist von ca. drei Monaten ausreichen, da ein Unternehmen für acht Wochen nach Zugang der Rechnung noch Beanstandungen bearbeiten muss (s. § 45i Absatz 1 TKG). Diese acht Wochen zuzüglich der Postlaufzeiten und der Bearbeitungszeit von Einwendungen beim Anbieter ergeben etwa drei Monate. Die Frist beginnt mit Versendung der Rechnung, d. h., wenn eine Rechnung verspätet gestellt wird, beginnt diese Frist erst später. Bei einer Beanstandung der Rechnung dürfen die Verkehrsdaten bis zur abschließenden Klärung gespeichert werden.

Um Beanstandungen durchzuführen, werden die Verkehrsdaten unabhängig davon gespeichert, ob ein Einzelverbindungsnachweis verlangt wird (s. Kapitel 2.9). Dies ermöglicht es, im Einzelfall einen nachträglichen Einzelverbindungsnachweis anzufordern. Es gibt noch einzelne Anbieter, die eine Löschung sämtlicher Verkehrsdaten nach Erstellung der Rechnung anbieten. Diese datenschutzfreundliche Option musste bis Ende 2007 angeboten werden, ist aber im Rahmen einer Gesetzesänderung entfallen.

Verkehrsdaten, die nicht für die Abrechnung benötigt werden, sind zu löschen, wenn sie nicht für andere Zwecke erforderlich sind. Dies betrifft etwa *Flatrategespräche*. Bei einer echten Flatrate steht das Entgelt fest, ohne die Verkehrsdaten hierfür auszuwerten. Es gibt aber auch „unechte" Flatrates, die einer Begrenzung unterliegen, so dass die Verkehrsdaten ausgewertet werden müssen.

Netzbetreiber erheben Entgelte, wenn sie Gespräche von anderen Netzbetreibern entgegennehmen. Um hier eine Abrechnung durchzuführen, müssen die Verkehrsdaten der Gespräche, die zwischen Kundinnen und Kunden verschiedener Netzbetreiber geführt werden, gespeichert werden. Ein reines Aufaddieren der Gesprächsminuten ist in der Regel nicht ausreichend, da sonst eine Prüfung der Abrechnung nicht möglich wäre. Dieser Umstand ist auch für Telefonkunden relevant. Es bedeutet nämlich, dass selbst bei Nutzung einer Flatrate oder bei ankommenden Gesprächen Verkehrsdaten beim Anbieter gespeichert werden – wenn auch nicht für die Abrechnung mit der jeweiligen betroffenen Person.

Mobilfunk-Serviceprovider vermarkten Telekommunikationsdienste und übernehmen die Abrechnung mit der Kundschaft. Die Mobilfunk-Netzbetreiber übernehmen dabei die Erbringung des Dienstes. Die Verkehrsdaten werden für zwei Abrechnungen benötigt. Zum einen stellt der Netzbetreiber dem Serviceprovider die erbrachten Leistungen in Rechnung. Zum anderen gibt der Netzbetreiber die Verkehrsdaten an den Serviceprovider weiter, damit dieser wiederum die Leistungen seiner Kundschaft in Rechnung stellen kann. Auch in anderen Fällen, etwa bei der Erbringung von Mehrwertdiensten oder bei Call-by-Call Dienstleistungen, sind mehrere Anbieter beteiligt, so dass auch hier Verkehrsdaten an verschiedenen Stellen erhoben und verarbeitet werden.

2.8 Ortung und Standortdaten

Die heutigen, aus Funkzellen bestehenden, Mobilfunknetze benötigen Standortdaten der eingebuchten Handys, damit die Teilnehmerin bzw. der Teilnehmer erreichbar sind und mobil telefonieren, SMS versenden, chatten oder im Internet surfen können. So entstehen bei einer normalen Handynutzung Standortdaten. Bei standortabhängigen

Tarifen müssen diese für die Abrechnung gespeichert werden, um feststellen zu können, welche Gespräche z. B. im günstigeren Heimatbereich geführt wurden.

Darüber hinaus können die Standortdaten auch für andere praktische Dienste verwendet werden. Sie erleichtern die Restaurantsuche und helfen einem Spediteur festzustellen, ob sein Lastkraftwagen (LKW) noch im Stau auf der Autobahn steht oder schon bei der Kundschaft angekommen ist. Aber die Standortdaten können auch dazu missbraucht werden, andere Menschen ohne deren Wissen und Zustimmung zu überwachen.

Das TKG regelt nur den Umgang mit Standortdaten, die im Rahmen der Telekommunikation von den Netzbetreibern erfasst werden. Dies ist insbesondere der Fall, wenn ein Mobilfunknetz feststellt, in welcher Funkzelle sich das Handy befindet. Dadurch kann auch ein einfaches klassisches Handy geortet werden. Die hier aufgeführten Regelungen würden aber auch für einen Dienst gelten, bei dem der Standort über Satellitenortung festgestellt, aber für einen Telekommunikationsdienst verwendet wird. Die Fallkonstellation, dass die Standortdaten nicht von einem Telekommunikationsnetz oder Telekommunikationsdienst erhoben oder verwendet werden, wird in Kapitel 4.2.4 erläutert.

In § 98 TKG werden Regelungen getroffen, die einen Missbrauch der Dienste verhindern sollen, ohne jedoch überflüssige Hürden bei der Nutzung des Dienstes aufzubauen. Die Anzahl der hier zu unterscheidenden Fälle macht die Thematik recht komplex.

Wenn der Standort an Dritte übermittelt werden soll, ist vor der ersten Ortung eine ausdrückliche, gesonderte und schriftliche Einwilligung gegenüber dem Ortungsdiensteanbieter erforderlich. Weiterhin ist bei jeder Ortung eine Textmitteilung, d. h. eine SMS, an das geortete Handy zu schicken. Durch die schriftliche Einwilligung soll ein Missbrauch erschwert werden. Ferner wird dem Teilnehmer bewusst, dass er eine weitgehende Einwilligung tätigt, was bei einem Klick am Handy nicht unbedingt der Fall wäre. Sollte eine Einwilligung dennoch gefälscht werden, fällt die Ortung durch den Empfang der SMS auf.

Wenn der Teilnehmer, d. h. der Vertragspartner des Mobilfunkanbieters, selbst sein Handy ortet, entfällt die Forderung nach einer schriftlichen Einwilligung. Ein hierfür typischer Dienst wäre die Ortung eines vergessenen oder verlorenen Handys.

Bei der Ortung von Firmenhandys muss das Unternehmen zwar nicht unbedingt die schriftliche Einwilligung der betroffenen Beschäftigten einholen, aber auch hier gelten die datenschutzrechtlichen Grundsätze der Transparenz und Verhältnismäßigkeit. Neben mitbestimmungsrechtlichen Regelungen ist die Verpflichtung im TKG zu beachten, dass der *Teilnehmende* (hier: das Unternehmen) den *Mitbenutzende* (hier: das Personal) über die Einwilligung zu informieren hat. Darüber hinaus ist auch wieder eine SMS bei jeder Ortung zu versenden. Insofern würde es schnell auffallen, wenn die Information der Mitbenutzenden „vergessen" werden sollte. Die Versendung der SMS ist dann entbehrlich, wenn der Standort nur auf dem Handy angezeigt wird. Diese SMS würde nur Kosten verursachen und den Nutzenden stören, ohne dass eine Missbrauchsgefahr besteht. Eine einfache Einwilligung – z. B. per Klick am Handy – ist ausreichend. Selbstverständlich muss es auch möglich sein, eine Einwilligung zur Ortung jederzeit zu widerrufen.

2.9 Einzelverbindungsnachweis

Viele Kundinnen und Kunden haben ein berechtigtes Interesse daran, nach Erhalt ihrer Telefonrechnung die Richtigkeit der Entgelte zu überprüfen und die Entstehung der einzelnen Kosten nachzuvollziehen. Zu diesem Zweck können sie den sog. *Einzelverbindungsnachweis* (EVN) verlangen, eine nach Einzelverbindungen aufgeschlüsselte Rechnung, auf die die Kundinnen und Kunden einen gesetzlichen Anspruch haben (§ 45e Absatz 1 Satz 1 TKG).

§ 99 Absatz 1 Satz 1 TKG sieht vor, dass der Diensteanbieter den Kundinnen und Kunden die entgeltpflichtigen Verkehrsdaten mitteilen muss, wenn diese vor dem maßgeblichen Abrechnungszeitraum in Textform einen EVN verlangt haben. Da immer mehr Kundinnen und Kunden im Rahmen einer sog. *Flatrate* telefonieren und dennoch einen Nachweis der Verbindungen wünschen, hat der Gesetzgeber in § 99 Absatz 1 Satz 1 TKG die Möglichkeit eröffnet, auf Wunsch den Kundinnen und Kunden auch die einzelnen

Daten pauschal abgegoltener Verbindungen mitteilen zu können. Allerdings besteht hier kein Anspruch, sondern der Diensteanbieter entscheidet, ob er diesem Kundenwunsch nachkommt oder nicht.

Aus dem Standard-EVN ergeben sich alle Daten von solchen Verbindungen, die entgeltpflichtig sind. Folgenden daten- und verbraucherschutzrechtlichen Anforderungen muss ein EVN genügen:

- Der Standard-EVN muss kostenfrei angeboten werden;
- Datum und Anschlussnummer der Kundin/des Kunden müssen angegeben werden;
- die Zielrufnummer ist – je nach Wunsch der Kundinnen und Kunden – vollständig anzugeben oder um die letzten drei Ziffern zu verkürzen (§ 99 Absatz 1 Satz 2 TKG);
- Beginn und Ende der Verbindung oder die Dauer sind notwendige Angaben und
- die jeweilige Tarifeinheit oder das Entgelt für das einzelne Gespräch müssen angegeben werden.

Kundinnen und Kunden, die zur vollständigen oder teilweisen Übernahme der Entgelte für eingehende Gespräche verpflichtet sind, dürfen im EVN die Nummern der Anschlüsse, von denen die Anrufe ausgehen, nur unter Kürzung der letzten drei Ziffern mitgeteilt werden (§ 99 Absatz 1 Satz 7 TKG). Hiermit soll verhindert werden, dass die Anbieter von Werbeplattformen quasi automatisch die Rufnummern ihrer Gesprächspartner erfahren, die sie – etwa über die Inverssuche in Telefonverzeichnissen (s. Kapitel 2.14) – sogar namentlich zuordnen können.

Darüber hinaus gibt es in § 99 Absatz 1 Sätze 3 und 4 TKG noch folgende gesetzliche Vorgaben zum EVN:

Mitbenutzerschutz

Bei Anschlüssen im Privathaushalt müssen die Kundinnen und Kunden schriftlich erklärt haben, alle zum Haushalt gehörenden Personen, die den Anschluss mitnutzen, darüber informiert zu haben und künftige Mitbenutzende unverzüglich über die Verwendung von EVN zu informieren. Bei Anschlüssen in Betrieben und Behörden muss die auftraggebende Person schriftlich erklärt haben, dass die Mitarbeiterinnen und Mitarbeiter informiert worden seien, künftige Beschäftigte informiert würden und

der Betriebsrat bzw. der Personalrat entsprechend den gesetzlichen Vorschriften beteiligt worden oder eine solche Beteiligung nicht erforderlich sei. Dieser Mitbenutzerschutz gilt auch dann, wenn ein Arbeitgeber seinen im Außendienst beschäftigten Mitarbeiterinnen und Mitarbeitern Firmenmobiltelefone zur Verfügung stellt. Deren Zustimmung ist – unabhängig davon, ob nur geschäftliche oder auch private Nutzung des Anschlusses zugelassen ist – im Regelfall nicht erforderlich.

Anonyme Kommunikation

§ 99 Absatz 2 TKG regelt die Besonderheit von Telefonaten zu Anschlüssen von Personen, Behörden und Organisationen, die der anonymen Beratung im sozialen oder kirchlichen Bereich dienen. Diese Verbindungen dürfen im EVN nicht enthalten sein. Dadurch wird die anonyme Kommunikation als unerlässliche Voraussetzung für die Arbeit der genannten Einrichtungen gesichert. Geschützt sind neben Anrufen bei der Telefonseelsorge auch solche bei Ehe-, Familien-, Erziehungs- oder Jugendberatern sowie Beratern für Suchtfragen und bei der Gesundheitsberatung. Die BNetzA nimmt die betreffenden Anschlüsse in eine Liste auf, die zum Abruf im automatisierten Verfahren den Diensteanbietern bereitgestellt wird. Diese sind verpflichtet, die Liste quartalsweise abzufragen und Änderungen unverzüglich in den Abrechnungsverfahren anzuwenden.

2.10 Störungsbeseitigung und Missbrauchserkennung

§ 100 TKG erlaubt Telekommunikationsdiensteanbietern, Bestands- (s. Kapitel 2.5) und Verkehrsdaten (s. Kapitel 2.6) zu verarbeiten, um Störungen in oder Missbrauch von ihren Systemen aufzudecken und zu unterbinden.

Störungsbeseitigung

Beim Betrieb von Telekommunikationsanlagen können vielfältige Probleme und Störungen auftreten. Um einen fehlerfreien Betrieb zu gewährleisten, analysieren Diensteanbieter Verkehrsdatenflüsse. Sie dürfen gemäß § 100 Absatz 1 TKG für diesen Zweck Verkehrsdaten erheben und verwenden. Die BfDI hält – in Anlehnung an ein Urteil des Bundesgerichtshofs vom 13. Januar 2011 – grundsätzlich eine Speicherfrist von bis zu sieben Tagen für vertretbar.

Seit Mitte 2017 ist im Gesetz zudem explizit geregelt, dass neben Bestands- und Verkehrsdaten auch die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung für diese Zwecke genutzt werden können (s. auch Kapitel 4.4.1). Die Steuerdaten eines informationstechnischen Protokolls dienen der Kommunikation zwischen Anwendungen und Servern, etwa damit eine E-Mail übermittelt oder damit eine Internetseite vom Server zum Browser übertragen werden kann. Die Inhalte, z. B. der Text einer E-Mail, werden dabei nicht umfasst.

Soweit die Daten nicht automatisiert erhoben und verwendet werden, gibt es eine quartalsweise Berichtspflicht gegenüber der BfDI und der BNetzA. Außerdem besteht eine Benachrichtigungspflicht gegenüber dem Betroffenen, falls dieser ermittelt werden kann.

Sofern erforderlich, kann sich der Diensteanbieter zur Störungsbeseitigung nach § 100 Absatz 2 TKG im Ausnahmefall sogar auf einzelne Gespräche aufschalten. In diesem Fall muss das Aufschalten auf die Verbindung den Kommunikationsteilnehmern durch ein akustisches oder sonstiges Signal angezeigt werden. In Fällen, in denen eine Signalisierung des Mithörens aus technischen Gründen nicht möglich ist, muss der oder die betriebliche Datenschutzbeauftragte des Unternehmens in das Verfahren eingebunden werden.

Missbrauchserkennung

Ein weiterer Grund für eine Bestands- und Verkehrsdatenauswertung durch Diensteanbieter ist das Aufdecken und Unterbinden von missbräuchlicher Nutzung der von ihnen angebotenen Dienste. So erlaubt § 100 Absatz 3 TKG die Verwendung von Verkehrsdaten, um beispielsweise Leistungserschleichungen oder Betrug festzustellen. Dabei muss der Zweck der Datennutzung ausschließlich auf die Identifizierung und Verhinderung solcher rechtswidrigen Inanspruchnahmen beschränkt sein, die zu Lasten des jeweiligen Diensteanbieters gehen.

Zur Missbrauchserkennung darf ein Unternehmen die aus anderen Gründen rechtmäßig gespeicherten Verkehrsdaten analysieren, die nicht älter als sechs Monate sind. Sollten darüber hinaus noch weitere Verkehrsdaten benötigt werden, für deren Verwendung keine eigene Rechtsgrundlage existiert, können diese für bis zu sieben Tage

gespeichert werden. Sobald im Rahmen der Datenanalyse tatsächliche Anhaltspunkte für einen Missbrauchsfall festgestellt werden, können die hiermit in Zusammenhang stehenden Daten so lange gespeichert bleiben, wie es zur Bearbeitung des Falles erforderlich ist. Die festgestellten Anhaltspunkte sind vom Diensteanbieter revisionssicher zu dokumentieren.

2.11 Fangschaltung

Durch das Fangschaltverfahren nach § 101 TKG soll Teilnehmenden, die belästigende oder bedrohende Anrufe erhalten, ermöglicht werden, den Anschluss festzustellen, von dem diese Anrufe ausgehen. Insbesondere bei unterdrückten Rufnummern stellt eine Fangschaltung oft die einzige Möglichkeit dar, die Quelle für solche Anrufe zu identifizieren, um dann entsprechende straf- oder zivilrechtliche Schritte einzuleiten.

Anspruchsvoraussetzungen und Verfahren

Um eine Fangschaltung einrichten zu lassen, müssen Beteiligte gegenüber dem Diensteanbieter schriftlich darlegen, dass auf dem Anschluss bedrohende oder belästigende Anrufe ankommen. Dieser überprüft lediglich die Schlüssigkeit des Antrages, nicht jedoch, ob die vorgetragene Bedrohungslage oder Belästigung tatsächlich vorliegt.

Sofern ein entsprechender Antrag vorliegt, sichert der Diensteanbieter die Rufnummern, Namen und Anschriften der Inhaber dieser Anschlüsse sowie Datum und Uhrzeit des Beginns der Verbindungen und Verbindungsversuche von sämtlichen auf dem überwachten Anschluss eingehenden Anrufen. Diese werden allerdings nicht vollumfänglich an den Teilnehmenden herausgegeben. Vielmehr muss dieser nach geeigneten Kriterien (z. B. Datum und Uhrzeit) eingrenzen, wann belästigende oder bedrohende Anrufe bei ihm eingegangen sind. Nur die Informationen zu den in diesen Zeitraum fallenden Verbindungen werden Betroffenen mitgeteilt; der Diensteanbieter dokumentiert das gesamte Verfahren.

Information der „gefangenen" Anschlussinhaber

Inhabende des Anschlusses, von denen die festgestellten Verbindungen ausgegangen sind, werden nach Abschluss des Verfahrens darüber informiert, dass die Daten unter

den oben genannten Voraussetzungen einem Dritten mitgeteilt wurden. Von einer solchen Benachrichtigung kann abgesehen werden, wenn die antragstellende Person schriftlich und schlüssig dargelegt hat, dass daraus wesentliche Nachteile entstehen könnten, sollten die Inhabenden der so festgestellten Anschlüsse informiert werden. In diesem Fall hat der Diensteanbieter abzuwägen, ob die von der antragstellenden Person dargelegten Nachteile das schutzwürdige Informationsinteresse der *„gefangenen"* Anschlussinhaber überwiegen.

Dauer der Fangschaltung

Bei der Dauer einer Fangschaltung ist zwischen einer Nutzung von Privatanschlüssen einerseits und Anschlüssen von Firmen oder öffentlichen Institutionen andererseits zu unterscheiden. Im privaten Bereich soll eine Fangschaltung für höchstens einen Monat installiert werden. Im geschäftlichen oder öffentlichen Umfeld darf die Dauer bei Vorliegen einer besonderen Bedrohungslage maximal sechs Monate betragen. Unter welchen Umständen eine entsprechende besondere Bedrohungslage vorliegt, ist sehr restriktiv zu beurteilen. In der Regel wird dies hauptsächlich bei gefährdeten öffentlichen oder infrastrukturellen Einrichtungen wie beispielsweise Flughäfen der Fall sein. Sofern nach Ablauf der jeweiligen Frist die Quelle für die bedrohenden oder belästigenden Anrufe nicht festgestellt worden konnte, diese aber weiterhin anhalten, kann die Fangschaltung verlängert werden. Dafür muss jedoch ein erneuter Antrag unter den oben genannten Voraussetzungen gestellt werden; keinesfalls darf die Fangschaltung zu einer Dauereinrichtung werden.

Keine präventive Fangschaltung

§ 101 TKG kann auch nicht als Rechtsgrundlage für eine präventive Fangschaltung herangezogen werden, z. B. im Vorfeld einer Großveranstaltung für potentielle Bombendrohungen. Hier wird es regelmäßig nicht möglich sein, Belästigungen oder Drohanrufe glaubhaft zu machen. Eine Überwachung der Verkehrsdaten (s. Kapitel 3.8) muss in diesen Fällen von den zuständigen Sicherheitsbehörden unter Berufung auf die entsprechenden Rechtsgrundlagen (z. B. § 100g StPO) angeordnet werden.

2.12 Rufnummernunterdrückung

Privat Nutzende haben das Recht, die Anzeige ihrer Rufnummer zu unterdrücken; wer werblich anruft, darf das hingegen nicht. Bei der Versendung einer SMS wird die Rufnummer hingegen als Bestandteil der Absenderadresse immer mit übertragen.

§ 102 Absatz 1 TKG regelt, dass Diensteanbieter, die die Anzeige der Rufnummer auf dem Display des Endgerätes anbieten, ihren Kundinnen und Kunden folgende Wahlmöglichkeiten einräumen müssen, soweit dies technisch möglich ist:

- Anrufende können die Anzeige der Nummer dauernd oder für jeden Anruf einzeln unterdrücken;
- Angerufene können die Anzeige der Nummer dauernd oder für jeden Anruf einzeln unterdrücken und
- Angerufene können Anrufe abweisen, wenn die Rufnummernanzeige vom Anrufenden unterdrückt wurde.

Diese Wahlmöglichkeiten müssen den Kundinnen und Kunden auf einfache Weise und unentgeltlich angeboten werden. Sie gelten gemäß § 102 Absatz 7 TKG auch für Anrufe in das Ausland und für aus dem Ausland kommende Anrufe, soweit sie Anrufende oder Angerufene im Inland betreffen. Aus verbraucherschutzrechtlichen Erwägungen hat der Gesetzgeber gemäß § 102 Absatz 2 TKG Anrufenden bei telefonischer Werbung ausdrücklich untersagt, die Rufnummernanzeige zu unterdrücken oder bei dem Diensteanbieter zu veranlassen, dass diese unterdrückt wird. Der werblich Anrufende hat sicherzustellen, dass die ihm zugeteilte Rufnummer dem Angerufenen übermittelt wird. Nach § 102 Absatz 4 Satz 1 TKG muss der Diensteanbieter auf Antrag des Kunden Anschlüsse bereitstellen, bei denen die Übermittlung des anrufenden Anschlusses an den angerufenen Anschluss unentgeltlich ausgeschlossen wird. Diese Anschlüsse sind auf Antrag der jeweiligen Kundinnen oder Kunden in dem öffentlichen Teilnehmerverzeichnis (§ 104 TKG) seines Diensteanbieters zu kennzeichnen (§ 102 Absatz 4 Satz 2 TKG). Ist eine solche Kennzeichnung erfolgt, so darf an den so gekennzeichneten Anschluss eine Übermittlung der Rufnummer des Anschlusses, von dem der Anruf ausgeht, erst dann erfolgen, wenn zuvor die Kennzeichnung in der aktualisierten Fassung des Teilnehmerverzeichnisses nicht mehr enthalten ist (§ 102 Absatz 4 Satz 3 TKG).

Bei Kundinnen und Kunden, die nicht in ein Teilnehmerverzeichnis eingetragen sind, muss nach § 102 Absatz 5 TKG die Anzeige der Rufnummer grundsätzlich unterbleiben. Die betreffenden Anschlussinhaber können allerdings ausdrücklich bestimmen, dass auch ohne eine Eintragung im Teilnehmerverzeichnis ihre Rufnummer beim Angerufenen angezeigt wird.

Für Verbindungen zu Anschlüssen mit den Rufnummern 110, 112, 116 117 (kassenärztlicher Bereitschaftsdienst) oder 124 124 (Seenotrettung) hat der Diensteanbieter sicherzustellen, dass eine Anzeige der Rufnummer in jedem Fall erfolgt (§ 102 Absatz 8 TKG).

2.13 Teilnehmerverzeichnisse

Gemäß § 104 TKG können Teilnehmer selbst bestimmen, ob und in welcher Form sie in ein öffentliches gedrucktes oder elektronisches Teilnehmerverzeichnis (Telefonbuch) eingetragen werden möchten. Telekommunikationsdiensteanbieter dürfen nur solche Einträge aufnehmen, die ausdrücklich beantragt wurden. Auch haben die Kundinnen und Kunden jederzeit das Recht, ihre Einträge ändern oder löschen zu lassen. Der Diensteanbieter hat den jeweiligen Kundenwunsch frühestmöglich umzusetzen.

Bei der Eintragung haben die Kundinnen und Kunden zahlreiche Gestaltungsrechte. Sie können entscheiden, ob und mit welchen Angaben (Name, Anschrift, Beruf, Branche, Art des Anschlusses) sie in öffentliche Verzeichnisse eingetragen werden möchten, und auch, ob die Eintragung nur in gedruckten oder in elektronischen öffentlichen Verzeichnissen oder in beiden erfolgen soll. Angaben über Mitbenutzende dürfen nur eingetragen werden, soweit diese sich damit einverstanden erklären (§ 104 Satz 3 TKG).

Bei einem Eintrag von Daten in öffentliche elektronische Kundenverzeichnisse sollte sich jeder darüber im Klaren sein, dass der Telefonanschluss über Internet-Dienste bekannt gegeben werden kann. Diese Daten können dann von Dritten mit Hilfe geeigneter Software ausgewertet werden. Hierdurch können unter Umständen vom Kunden nicht gewünschte, nicht erwartete oder sogar unzulässige Datenverknüpfungen vorgenommen werden.

Beachtet ein Diensteanbieter den Kundenwunsch nicht, verletzt er damit dessen schutzwürdige Interessen und muss mit datenschutzrechtlich vorgesehenen Sanktionen oder zivilrechtlichen Ansprüchen geschädigter Betroffener rechnen. So kann die betroffene Person bei Zuwiderhandlungen seine Interessen rechtlich durchsetzen. Nach § 7 BDSG hat er einen Rechtsanspruch auf Schadensersatz, wenn ihm eine verantwortliche Stelle einen Schaden zugefügt hat, und zwar durch eine nach dem BDSG oder nach anderen Vorschriften über den Datenschutz unzulässige Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten. Allerdings entfällt diese Schadensersatzpflicht, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat (§ 7 Satz 2 BDSG). Dies bedeutet, dass die Kundin oder der Kunde das schadensverursachende Ereignis und die Ursächlichkeit zwischen diesem Ereignis und dem eingetretenen Schaden nachweisen muss. Bei der Durchsetzung dieses Rechtsanspruches ist ausschließlich der zivile Rechtsweg gegeben.

2.14 Telefonauskunft

Nach § 105 Absatz 1 TKG darf im Einzelfall Auskunft über die in öffentlichen Kundenverzeichnissen enthaltenen Rufnummern erteilt werden (Telefonauskunft). Die Kundin bzw. der Kunde ist über die Wahl- und Gestaltungsmöglichkeiten zu den Einträgen über die eigenen Daten in diesen Verzeichnissen zu informieren.

Das TKG regelt in § 105 Absatz 2 Sätze 1 und 2, dass

- die Telefonauskunft über Rufnummern von Kundinnen und Kunden nur erteilt werden darf, wenn diese in angemessener Weise darüber informiert worden sind, dass sie der Weitergabe ihrer Rufnummer widersprechen können und hiervon keinen Gebrauch gemacht haben und
- über Rufnummern hinausgehende Auskünfte über nach § 104 TKG veröffentlichte Daten nur erteilt werden dürfen, wenn die betreffende Person in eine weitergehende Auskunftserteilung eingewilligt hat.

Die sog. *Inverssuche* regelt Absatz 3 der Norm: Namen und/oder Anschrift Teilnehmender, wo nur die Rufnummer bekannt ist, darf die Telefonauskunft nur weiter-

geben, wenn der in ein Teilnehmerverzeichnis eingetragene Betroffene nach einem Hinweis des Diensteanbieters auf das Widerspruchsrecht nicht widersprochen hat.
Ein Widerspruch nach Absatz 2 Satz 1 oder Absatz 3 oder eine Einwilligung nach Absatz 2 Satz 2 sind in den Kundendateien des Diensteanbieters und des Anbieters nach Absatz 1, die den Verzeichnissen zu Grunde liegen,

- gemäß § 105 Absatz 4 Satz 1 TKG *unverzüglich* zu vermerken und
- gemäß Satz 2 auch von den anderen Diensteanbietern zu beachten, sobald diese in zumutbarer Weise Kenntnis darüber erlangen konnten, dass sie in den Verzeichnissen des Diensteanbieters und des Anbieters nach Absatz 1 vermerkt ist.

Selbstverständlich können die Kundinnen und Kunden ihr Einverständnis jederzeit durch eine entsprechende Erklärung gegenüber dem Diensteanbieter zurückziehen; ebenso ist ein Widerspruch jederzeit möglich. Bei einem Anbieterwechsel müssen die Kundinnen und Kunden allerdings eine neue Entscheidung über die Verwendung ihrer Daten durch die Telefonauskunft treffen.

2.15 Notrufe

Werden Notrufnummern gewählt, sind oft Leben oder Gesundheit von Menschen in Gefahr. Deshalb wird bei Notrufen – anders als bei sonstigen Verbindungen – stets die Rufnummer und der Standort des Anrufers übermittelt (§ 108 TKG). Dies betrifft sowohl den Mobilfunk, bei dem Informationen zur Funkzelle übermittelt werden, als auch die Adresse eines Telefonanschlusses im Festnetz. Diese Daten werden vom Diensteanbieter an die Rettungsleitstelle übermittelt. Die Einzelheiten regeln die Notrufverordnung und die seit Dezember 2012 gültige Technische Richtlinie Notruf. In bestimmten Fällen, in denen mehrere Netzbetreiber mitwirken (wie z. B. bei der Internettelefonie), erfolgt die Umsetzung erst zu einem späteren Zeitpunkt.

Auch bei Anrufen zum kassenärztlichen Bereitschaftsdienst (116 117) dürfen die Rufnummer und der Standort übermittelt werden, da auch in diesen Fällen die Anrufe oft durch lebensbedrohliche Situationen ausgelöst werden.

2.16 Technische Schutzmaßnahmen

Jeder Anbieter von Telekommunikationssystemen ist dazu verpflichtet, das Fernmeldegeheimnis zu wahren und personenbezogene Daten seiner Kundschaft zu schützen. Die öffentlichen Telekommunikationssysteme (sowohl Mobilfunk- als auch Festnetze) sind nach der Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als sog. *Kritische Infrastruktur* (KRITIS) anzusehen. Dies sind Organisationen und (technische) Einrichtungen mit großer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Sowohl Netzbetreiber als auch Service-Provider müssen gemäß § 109 Absatz 1 TKG geeignete technische Schutzmaßnahmen treffen, um sowohl die Verfügbarkeit dieser Netze sicherzustellen als auch das Fernmeldegeheimnis und den Schutz von personenbezogenen Daten zu wahren; solche Schutzmaßnahmen sind nach dem Stand der Technik auszuführen. Diese Verantwortung verbleibt auch dann beim Diensteanbieter, wenn die Daten im Rahmen einer Auftragsdatenverarbeitung gemäß § 11 Absatz 1 BDSG im Auftrag durch eine andere Stelle erhoben, verarbeitet oder genutzt werden (s. Kapitel 3.3). Ergänzend hierzu sind die Betreiber Kritischer Infrastrukturen gemäß dem IT-Sicherheitsgesetz verpflichtet, IT-Sicherheit nach dem Stand der Technik umzusetzen und deren Einhaltung regelmäßig nachzuweisen.

Im Hinblick auf den technischen Schutz schreibt das Gesetz keine bestimmten Maßnahmen vor. Die geforderten technischen Vorkehrungen werden jedoch dann nach § 109 Absatz 2 TKG als angemessen angesehen, wenn der technische und wirtschaftliche Aufwand in Relation zu den zu schützenden Telekommunikationsnetzen und -diensten steht. Ergänzend zu diesen technischen Vorkehrungen werden gemäß § 109 Absatz 1 TKG auch „sonstige Maßnahmen“ gefordert. Darunter fällt z. B. die Festlegung von organisatorischen Schritten, die unternehmensinterne Abläufe und Prozesse beim Umgang mit personenbezogenen Daten definieren. Zur Umsetzung dieser Maßnahmen muss jeder Betreiber und Diensteanbieter eines öffentlichen Telekommunikationsnetzes einen Sicherheitsbeauftragten benennen. Zudem bedarf es eines Sicherheitskonzepts, das die technischen Vorkehrungen und sonstigen Schutzmaßnahmen beschreibt (§ 109 Absatz 4 Satz 1 TKG). Weiterhin hat die BNetzA im Benehmen mit dem BSI und der BfDI

einen Katalog von Sicherheitsanforderungen erstellt, den die BNetzA veröffentlicht (§ 109 Absatz 6 TKG) hat.

2.17 Meldepflicht bei datenschutzrelevanten Datensicherheitsvorfällen und Schadsoftware

§ 109a TKG verpflichtet Anbieter öffentlich zugänglicher Telekommunikationsdienste, Vorfälle zu melden, bei denen der Schutz der von ihnen verarbeiteten personenbezogenen Daten verletzt worden oder zu erwarten ist. Diese gesetzliche Informationspflicht ist zweigliedrig ausgestaltet.

Meldung an die Aufsichtsbehörden

Eine Meldung muss – unabhängig von den Umständen des zu meldenden Vorfalls – immer gegenüber der BNetzA und der BfDI erfolgen. Die Meldepflicht nach § 109a Absatz 1 Satz 1 TKG ist dabei unbeschränkt, so dass auch vermeintlich kleinere Vorfälle mit potentiell weniger schweren Auswirkungen den Aufsichtsbehörden mitzuteilen sind. Die BNetzA hat in Zusammenarbeit mit der BfDI Leitlinien im Sinne des § 109a Absatz 7 TKG erstellt, die das Verfahren der Meldung eines Datenschutzvorfalls erläutern und somit vereinfachen sollen; diese Leitlinien können über die Websites der jeweiligen Behörden abgerufen werden.

Benachrichtigung der Betroffenen

Neben der Meldung des Vorfalls an die Aufsichtsbehörden ist die umgehende Benachrichtigung der Betroffenen vorgesehen, sofern zu erwarten ist, dass diese hierdurch schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden. Mit der Benachrichtigung soll den Betroffenen ermöglicht werden, weitere Schritte einzuleiten, um die Folgen der Datenschutzverletzung vermeiden oder zumindest begrenzen zu können. Die Benachrichtigung muss deshalb Informationen erhalten zu:

- der Art der Datenschutzverletzung,
- Kontaktpersonen oder -stellen, bei denen die Betroffenen weitere Informationen erhalten können,

- Empfehlungen und Maßnahmen, die mögliche nachteilige Auswirkungen des Vorfalls begrenzen können.

Ausnahmsweise kann eine Benachrichtigung der Betroffenen entbehrlich sein, wenn die vom Datenschutzvorfall betroffenen Daten durch geeignete technische Vorkehrungen vor einer unberechtigten Kenntnisnahme geschützt sind, wie z. B. durch ein als sicher anerkanntes Verschlüsselungsverfahren. Um beurteilen zu können, ob die Entscheidung auf eine Benachrichtigung zu verzichten, rechtmäßig getroffen wird, ist jeder Vorfall zwingend gegenüber BNetzA und BfDI zu melden. Unabhängig von der Pflicht zur Benachrichtigung der Betroffenen kann daher die Meldepflicht gegenüber den Aufsichtsbehörden nie entfallen.

Verzeichnis der Datenschutzverletzungen

Neben der Melde- und Benachrichtigungspflicht des § 109a Absatz 1 TKG wird den Diensteanbietern in Absatz 3 der Norm auferlegt, ein Verzeichnis über die meldepflichtigen Vorfälle zu führen. Darin sind sämtliche Vorfälle der letzten 5 Jahre aufzuführen und Angaben zu den Umständen und Auswirkungen der Verletzungen sowie zu den ergriffenen Abhilfemaßnahmen festzuhalten. Das Verzeichnis muss den Aufsichtsbehörden auf Anfrage zur Verfügung gestellt werden.

Schadsoftware

Seit Mitte 2017 sind Diensteanbieter zudem verpflichtet ihre Nutzerinnen und Nutzer darüber zu informieren, wenn sie feststellen, dass von deren Systemen Störungen ausgehen, die andere Telekommunikationsteilnehmer und eventuell sogar das Netz der Diensteanbieter beeinträchtigen. Dies kann beispielsweise der Fall sein, wenn jemand durch Schadsoftware auf dem Computer Teil eines sogenannten „Botnetz“ geworden ist. Betroffene Computer können dann beispielsweise dazu verwendet werden, ohne Wissen ihrer Besitzer Spam-E-Mails zu versenden oder andere Systeme anzugreifen. Die Diensteanbieter sind in diesen Fällen gehalten, den Betroffenen neben der Information über die Störung im zumutbaren Rahmen auch Hinweise zu geben, wie diese bestmöglich behoben werden kann. Sofern es zum Schutz der Systeme des Diensteanbieters erforderlich ist, darf dieser zudem den jeweiligen Nutzerinnen und Nutzern so lange den Zugang zum Netz verwehren, bis diese die Störung auf ihren Systemen beseitigt haben.

2.18 Technische Umsetzung von Überwachungsmaßnahmen

Die rechtlichen Grundlagen, die die inhaltliche Überwachung der Telekommunikation erlauben, sind nicht im TKG geregelt, sondern in verschiedenen Bundes- und Landesgesetzen, u. a.

- im Gesetz zu Artikel 10 GG,
- in der Strafprozessordnung,
- im Außenwirtschaftsgesetz und
- in Landespolizeigesetzen zur Gefahrenabwehr.

§ 110 TKG regelt demgegenüber die technische Umsetzung der Überwachungsmaßnahmen. Gleichzeitig ermächtigt § 110 Absatz 2 TKG die Bundesregierung, eine Rechtsverordnung – die TKÜV – zu erlassen (s. Anhang 9), die u. a. folgende Sachverhalte beinhaltet:

- Anforderungen an die technischen Einrichtungen sowie an die organisatorische Umsetzung von Überwachungsmaßnahmen mittels dieser Einrichtungen,
- das Genehmigungsverfahren und das Verfahren der Abnahme sowie
- Bestimmungen, nach denen bei Telekommunikationsanlagen aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit keine technischen Einrichtungen vorzuhalten sind.

Die TKÜV verpflichtet die Betreiber von Telekommunikationsanlagen, die ihre Dienste gegenüber jedermann anbieten, technische Einrichtungen zur Umsetzung der gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und vorbereitende organisatorische Vorkehrungen für die Umsetzung dieser Maßnahmen zu treffen. Diese Pflicht richtet sich aber nicht an die Betreiber von Telekommunikationsanlagen, die ihre Dienste nicht für die Öffentlichkeit, sondern nur für bestimmte Dritte anbieten. Hierzu zählen etwa die Nebenstellenanlagen in Hotels, Betrieben oder Krankenhäusern.

Weiterhin regelt die TKÜV die Vorkehrungen für die Erteilung von Auskünften über Verkehrsdaten. Dies beinhaltet sowohl Auskünfte über für betriebliche Zwecke ge-

speicherte Verkehrsdaten, als auch über aufgrund von § 113b TKG gespeicherte Daten (Vorratsdatenspeicherung).

Die Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR TKÜV) regelt die technischen und organisatorischen Details. Hier wird auch festgelegt, wie Anordnungen und Abfragen von Bestands- und Verkehrsdaten zwischen den Sicherheitsbehörden und den TK-Anbietern – jenseits der bisher oft üblichen Übermittlung per Telefax – übermittelt werden können. Dabei sollen keine automatisierten Abfragen durchgeführt werden, eine Prüfung der Anordnung durch den Anbieter ist hier vorgesehen.

2.19 Bestandsdaten für Sicherheitsbehörden

Gemäß § 111 TKG sind Telekommunikationsdiensteanbieter verpflichtet, bestimmte Bestandsdaten (s. Kapitel 2.5) für Auskunftsersuchen von Sicherheitsbehörden bereitzuhalten. Grundsätzlich handelt es sich dabei um Daten, die von den Unternehmen ohnehin für betriebliche Zwecke erhoben und vorgehalten werden. Allerdings muss deren Verfügbarkeit gewährleistet werden, z. B. für das automatisierte Auskunftsverfahren nach § 112 TKG (s. Kapitel 2.20).

Konkret sind gemäß § 111 Absatz 1 TKG die folgenden Daten zu erheben:

- Rufnummern und andere Anschlusskennungen,
- Name und Anschrift des Anschlussinhabers,
- bei natürlichen Personen deren Geburtsdatum,
- bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
- bei Mobilfunkanschlüssen, bei denen auch ein mobiles Endgerät überlassen wird, die Gerätenummer dieses Gerätes,
- das Datum des Vertragsbeginns und
- sobald bekannt, das Datum des Vertragsendes.
- Die Diensteanbieter haben darauf zu achten, dass die Daten korrekt und aktuell sind.

Vorab bezahlte Mobilfunkdienste

Seit dem 01. Juli 2017 müssen Kunden beim Kauf von Prepaid-SIM-Karten vor der Freischaltung entsprechender Dienste die Richtigkeit der erhobenen Daten anhand eines amtlichen Ausweisdokuments ggü. dem Anbieter nachweisen. Die entsprechende Ergänzung des § 111 TKG ist eine Maßnahme der Bundesregierung im Rahmen der Anti-Terror-Gesetzgebung. Die Bundesnetzagentur hat in diesem Zusammenhang eine Verfügung erlassen, wie diese Überprüfung im Einzelfall erfolgen muss. Die Telekommunikationsanbieter müssen bei im Voraus bezahlten Mobilfunkdiensten zudem Informationen zum verwendeten Überprüfungsverfahren sowie der Art, Nummer und ausstellenden Stelle des vorgelegten Legitimationsdokuments speichern.

2.20 Automatisiertes Auskunftsverfahren

§ 112 TKG regelt ein Verfahren, mit dem verschiedene, im Gesetz benannte öffentliche Stellen bestimmte Bestandsdaten über die BNetzA im Wege eines automatisierten Abrufs erlangen können.

Wer geschäftsmäßig Telekommunikationsdienste anbietet, ist nach § 112 TKG verpflichtet, die nach § 111 TKG erhobenen Daten zu speichern. Die Verpflichtung umfasst auch die Daten von Kundinnen und Kunden, die nicht in öffentlichen Verzeichnissen eingetragen sind. Die Kundendateien sind so verfügbar zu halten, dass die BNetzA einzelne Daten oder Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann.

Bedarfsträger, die Auskünfte aus den Kundendateien erhalten können, sind

- Gerichte und Strafverfolgungsbehörden,
- Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr,
- Zollkriminalamt und Zollfahndungsämter für Zwecke eines Strafverfahrens sowie das Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 23a des Zollfahndungsdienstgesetzes,

- Verfassungsschutzbehörden des Bundes und der Länder, Militärischer Abschirmdienst, Bundesnachrichtendienst,
- Notrufabfragestellen nach § 108 TKG sowie die Abfragestelle für die Rufnummer 124 124,
- Die Bundesanstalt für Finanzdienstleistungsaufsicht sowie
- Behörden der Zollverwaltung für die in § 2 Absatz 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen.

Die Auskünfte sind den Bedarfsträgern jederzeit unentgeltlich zu erteilen, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Die BNetzA hat die Daten, die in Kundendateien gespeichert sind, auf Ersuchen der vorgenannten Stellen automatisiert abzurufen und ihnen zu übermitteln.

Zum Zeitpunkt der Drucklegung dieser Broschüre konnten nur Rufnummern bzw. Name und Adresse der Teilnehmerinnen und Teilnehmer abgefragt werden. § 112 TKG erlaubt eine komplexere Abfrage nach unvollständigen Daten, etwa wenn nur Teile des Namens oder nicht die genaue Schreibweise (z. B. Maier oder Meyer) bekannt sind. Auch werden weitere Daten, etwa das Geburtsdatum oder die zum Anschluss gehörende E-Mail-Adresse übermittelt. Dies wird in der Kundendatenauskunftsverordnung (KDAV) geregelt; eine entsprechende Technische Richtlinie soll deren Umsetzung regeln.

Ferner haben die Telekommunikationsdiensteanbieter durch technische und organisatorische Maßnahmen sicherzustellen, dass sie von den Abrufen keine Kenntnis erlangen können. Damit soll vermieden werden, dass sie Spekulationen über die Zuverlässigkeit der betroffenen Kunden anstellen und ihnen vorsichtshalber den Vertrag kündigen nach dem Motto: „Wenn sich die BNetzA für XY interessiert, bedeutet das nichts Gutes“.

Die BNetzA gibt die abgerufenen Daten an die ersuchende Stelle weiter und protokolliert gemäß § 112 Absatz 4 TKG den Zeitpunkt des Abrufs, die für den Abruf verwendeten Daten, die abgerufenen Daten, die die Daten abrufende Person sowie die ersuchende Stelle und deren Aktenzeichen. Die Protokollierung soll eine genaue Datenschutzkontrolle ermöglichen. Ruft die BNetzA Daten für die Polizei eines Bundeslandes ab, kann der zuständige Landesdatenschutzbeauftragte bei der Polizei kontrollieren, ob die Abfrage zulässig war. Die BNetzA wiederum wird von der BfDI hinsichtlich der daten-

schutzrechtlichen Verpflichtungen kontrolliert. Im Gegensatz zu dem Verfahren nach § 113 TKG dürfen die Anbieter für Abfragen nach § 112 Absatz 5 Satz 3 TKG den Bedarfsträgern und der BNetzA keine Kosten in Rechnung stellen.

2.21 Manuelles Auskunftsverfahren

Neben diesem automatisierten Auskunftsverfahren sind die Diensteanbieter auch verpflichtet, manuelle Auskunftsersuchen von Sicherheitsbehörden zu beantworten. Die Auskunftspflicht betrifft dabei ausschließlich Bestandsdaten im Sinne der §§ 95 und 111 TKG (s. Kapitel 2.5 und 2.19).

Bestandsdatenauskunft und Doppeltürenmodell

§ 113 TKG verpflichtet Telekommunikationsdiensteanbieter, Auskunftsersuchen berechtigter Stellen über Bestandsdaten zu beantworten. So müssen beispielsweise Name und Anschrift des Inhabers einer konkreten Rufnummer herausgegeben oder andersherum Auskunft über die Rufnummer einer bestimmten Person erteilt werden. Auch Zugangssicherungscodes wie die PIN und PUK einer SIM-Karte oder das Zugangspasswort eines E-Mailkontos sind Gegenstand der Auskunftspflicht.

Die berechtigten Stellen müssen Auskunftsbegehren in Textform an den Diensteanbieter richten und dabei die entsprechende eigene Rechtsgrundlage angeben. § 113 TKG selbst stellt keine Rechtsgrundlage für das Auskunftsersuchen dar, wie das BVerfG in seinem Beschluss vom 24. Januar 2012 ausdrücklich klargestellt hat. Die verfassungsrechtliche Notwendigkeit, ein Auskunftsersuchen für die korrespondierenden Eingriffe durch Datenabfrage und -übermittlung jeweils auf eine eigenständige normenklare Rechtsgrundlage stützen zu müssen, bezeichnete das Gericht als sog. Doppeltürenmodell. Danach stehen zwischen der auskunftsersuchenden Stelle und dem auskunftserteilenden Telekommunikationsdiensteanbieter zwei Türen, die nur geöffnet sind, wenn im Einzelfall sowohl eine Ermächtigungsgrundlage für das Auskunftsersuchen als auch für die Auskunftserteilung existieren. Letztere findet sich grundsätzlich in § 113 TKG, während erstere in den jeweiligen Fachgesetzen, wie z. B. der Strafprozessordnung (s. Kapitel 3.8) geregelt sind.

Berechtigte Stellen

§ 113 Absatz 3 TKG beschränkt das Auskunftsverfahren auf die folgenden Stellen:

- Strafverfolgungs- und Bußgeldbehörden,
- Behörden mit Aufgaben zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung,
- Verfassungsschutzbehörden des Bundes und der Länder,
- Bundesnachrichtendienst,
- Militärischer Abschirmdienst.

IP-Adressen

§ 113 Absatz 1 Satz 3 TKG stellt ausdrücklich klar, dass die Auskunftspflicht auch Informationen zum Inhaber eines Anschlusses umfasst, dem zu einem bestimmten Zeitpunkt eine dynamische Internet-Protocol (IP)-Adresse zugeordnet war. Obwohl bei dieser Art von Auskunftsersuchen lediglich Bestandsdaten wie Name, Anschrift, Geburtsdatum, etc. übermittelt werden, war es lange streitig, ob das manuelle Bestandsdatenauskunftsverfahren derartige Auskünfte umfasst. Denn auch wenn sie nicht dem Anfragenden mitgeteilt werden, muss der Dienstesanbieter zur Feststellung der Zuordnung einer IP-Adresse intern Verkehrsdaten auswerten. Wie das BVerfG in seinem Beschluss klargestellt hat, umfasst das Auskunftsverfahren des § 113 TKG auch die Auskunft über den Anschlussinhaber einer IP-Adresse.

Diese sog. IP-Auskunft bleibt den in § 113 Absatz 3 TKG benannten Stellen vorbehalten. (Private) Rechteinhaber können ein Auskunftsersuchen nicht auf diese Norm stützen und müssen stattdessen auf das Verfahren nach § 101 UrhG (s. Kapitel 3.7) zurückgreifen.

Prüfpflichten der Telekommunikationsanbieter

§ 113 Absatz 2 Satz 3 TKG stellt klar, dass die Prüfung der materiellen Zulässigkeit eines Auskunftsersuchens ausschließlich unter die Verantwortlichkeit der abfragenden Stelle fällt. Die Diensteanbieter müssen lediglich das Vorliegen formeller Voraussetzungen (Textformerfordernis, ausdrückliche Benennung der Rechtsgrundlage für die Abfrage, ggf. richterliche Anordnung, etc.) kontrollieren. Nur wenn diese vorliegen, darf dem Ersuchen entsprochen und die begehrte Auskunft erteilt werden.

2.22 Aufsicht

Die datenschutzrechtliche Aufsicht über die Einhaltung der Vorschriften des TKG obliegt zwei Behörden, zum einen der generell für die Kontrolle und Durchsetzung der Vorschriften des TKG zuständigen BNetzA und zum anderen nach § 115 Absatz 4 TKG der BfDI. Diese tritt dabei an die Stelle der sonst nach § 38 BDSG zuständigen Landesbehörden, denen grundsätzlich die Aufsicht über den gesamten nicht-öffentlichen Bereich obliegt. Aus dieser klar geregelten Kompetenzabgrenzung folgt allerdings nicht, dass Telekommunikationsunternehmen ausschließlich der Datenschutzaufsicht der BfDI unterliegen. Diese hat lediglich die Aufgabe, die Einhaltung datenschutzrechtlicher Vorschriften des TKG zu überwachen. Diese regeln jedoch nur Aspekte der Verarbeitung der Daten von Teilnehmenden und Nutzenden der Telekommunikationsdiensteanbieter (s. Kapitel 2.2). Die Verarbeitung z. B. von Beschäftigtendaten dieser Unternehmen oder personenbezogener Daten von „Nicht-Kunden", wie z. B. Interessentendaten oder Daten, die im Rahmen einer Gewinnspielaktion erhoben wurden, unterliegen der Aufsicht der zuständigen Landesbehörden; eine Übersichtsliste findet sich in den Anhängen 11 und 12.

Kontroll- und Beanstandungsrecht

Anders als die BNetzA, die beispielsweise bei Gesetzesverstößen Bußgeldverfahren einleiten, Anordnungen treffen oder andere aufsichtsrechtliche Maßnahmen ergreifen kann, sind die Kompetenzen der BfDI bisher eingeschränkt. Zwar hat diese die Aufgabe, Telekommunikationsdiensteanbieter zu kontrollieren, sollte sie hierbei jedoch einen Verstoß feststellen, so kann dieser nur gegenüber der BNetzA beanstandet, nicht jedoch ein Bußgeld gegen den Anbieter verhängt werden. Da die ab dem 25. Mai 2018 anwendbare DSGVO klare Regelungen beinhaltet, welche Kompetenzen einer unabhängigen Datenschutzaufsichtsbehörde zukommen müssen, ist jedoch damit zu rechnen, dass in diesem Bereich entsprechende Anpassungen zu erwarten sind.

Beratungsfunktion und Petitionsrecht

Neben ihrer Kontrollfunktion berät die BfDI die Unternehmen der Telekommunikationsbranche in datenschutzrechtlichen Fragen, etwa bei der Einführung neuer Dienste und Angebote. Eine besonders wichtige Aufgabe ist, Eingaben von Bürgerinnen und Bürgern zu bearbeiten. Wer annimmt, bei der Erhebung, Verarbeitung oder Nutzung sei-

ner persönlichen Daten durch ein Telekommunikationsunternehmen in seinen Rechten verletzt worden zu sein, kann sich an die BfDI wenden (§ 21 BDSG). Als unabhängige Beschwerdeinstanz mit den o. g. Kontrollbefugnissen geht die BfDI den Beschwerden nach und unterrichtet die Betroffenen vom Ergebnis. Alle Eingaben werden vertraulich behandelt. Auf Wunsch der Betroffenen bleibt gegenüber den Telekommunikationsunternehmen der Name ungenannt, jedenfalls, solange eine anonyme Bearbeitung des Anliegens möglich ist. Zudem veröffentlicht die BfDI alle zwei Jahre einen Tätigkeitsbericht, der auch Beiträge aus dem Telekommunikationsbereich umfasst; die Tätigkeitsberichte können auf der Website abgerufen werden.

3 Sonstige bereichsspezifische Normen

3.1 Einwilligung nach § 4a BDSG

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein sog. Verbot mit Erlaubnisvorbehalt, d. h., sie sind verboten, wenn nicht

- eine Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet oder
- Betroffene dazu die Einwilligung erklären.

Wenn eine Rechtsvorschrift den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die Einwilligung von Betroffenen nicht an. Soll eine Einwilligung Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, ist folgendes zu beachten:

- Die Einwilligung muss tatsächlich freiwillig sein;
- die Einwilligung bedarf grundsätzlich der Schriftform; davon darf nur abgewichen werden, wenn wegen besonderer Umstände eine andere Form angemessen ist;
- Betroffene sind vorher über Umfang und Tragweite der Einwilligung aufzuklären (insbesondere über den Verarbeitungszweck und die verantwortliche Stelle);
- sie sind auch darüber zu informieren, was geschieht, wenn sie nicht einwilligen (z. B. dass Ansprüche verloren gehen können), soweit nach den Umständen des Einzelfalls erforderlich oder wenn sie dies verlangen.

Die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen, also frei von Zwang sein. Dabei ist auch zu berücksichtigen, ob sich Betroffene in einem besonderen Abhängigkeitsverhältnis (z. B. Arbeitsverhältnis) befinden oder ob aufgrund einer faktischen Situation (beispielsweise Monopolstellung desjenigen, der die Einwilligung einholen will) ein Zwang besteht. Bei der Verarbeitung *besonderer Arten*

personenbezogener Daten gemäß § 3 Absatz 9 BDSG (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) muss sich die Einwilligung ausdrücklich auf diese Daten beziehen. Besonders geregelt hat der Gesetzgeber die Einwilligung zu Werbezwecken (s. Kapitel 3.4).

3.2 Datenübermittlung ins Ausland nach §§ 4b und 4c BDSG

Für die Datenübermittlung ins Ausland gelten besondere Regelungen. Der Datenverkehr zwischen den Mitgliedstaaten der Europäischen Union – also innerhalb des europäischen Binnenmarktes – und mit den anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum im Anwendungsbereich des Unionsrechts ist genauso zu behandeln wie der inländische (§ 4b Absatz 1 BDSG).

Die Datenübermittlung in ein Land außerhalb der Europäischen Union, ein sog. Drittland, ist zulässig, wenn Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung haben, insbesondere, wenn in dem Drittland ein angemessenes Datenschutzniveau gewährleistet ist.

Ob dies der Fall ist, kann festgestellt werden:

- durch die verantwortliche Stelle selbst, die Daten übermitteln will, nach den Kriterien „Art der Daten, Zweckbestimmung, Dauer der geplanten Verarbeitung, Herkunft und Bestimmungsland, für den Empfänger geltende Rechtsnormen, Standesregeln und Sicherheitsmaßnahmen“ (§ 4b Absatz 3 BDSG),
- durch Adäquanzentscheidung der Europäischen Kommission nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG (so bisher geschehen für Andorra, Argentinien, Färöer, Guernsey, Israel, Isle of Man, Jersey, Kanada, Neuseeland, Uruguay und die Schweiz, sowie für Unternehmen in den Vereinigten Staaten von Amerika (USA), die sich im Rahmen des *EU-US Privacy Shields* zertifiziert haben).

Die Adäquanzentscheidung zum *EU-US Privacy Shield* basiert auf Verhandlungen zwischen der Europäischen Kommission und den USA und führt dazu, dass bei den nach den

Regeln des Privacy Shields zertifizierten Unternehmen seitens der EU ein angemessenes Niveau zur Verarbeitung personenbezogener Daten als gewährleistet betrachtet wird. Er tritt damit die Nachfolge der zuvor bestehenden *Safe Harbor*-Entscheidung der Europäischen Kommission an, die der EuGH mit seinem Urteil vom 6. Oktober 2015 (C-362/14) aufgehoben hatte.

Darüber hinaus kommt eine Übermittlung an einen Drittstaat auch im Rahmen abschließend aufgeführter und grundsätzlich eng auszulegender Ausnahmeregelungen in Betracht (§ 4c Absatz 1 BDSG). Möglich ist auch die Genehmigung der Übermittlung durch die zuständige Datenschutzaufsichtsbehörde; im Bereich der Telekommunikation ist die BfDI zuständig (§ 4c Absatz 2 BDSG). Hierfür können die verantwortlichen Stellen auch auf Standardvertragsklauseln für die Übermittlung (Standard Contractual Clauses) zurückgreifen oder sich selbst verbindliche Unternehmensregeln (Binding Corporate Rules) geben, die dann in einem Verfahren unter Einbindung anderer europäischer Aufsichtsbehörden als ausreichende Garantien anerkannt werden.

3.3 Auftragsdatenverarbeitung nach § 11 BDSG

Viele Telekommunikationsunternehmen bedienen sich Dritter bei der Erbringung und Abwicklung ihrer Dienste. Entschließt sich ein Unternehmen zum Outsourcing von Tätigkeiten, die die Erhebung, Verarbeitung und Nutzung personenbezogener Daten beinhalten, muss es zahlreiche rechtliche, technische und organisatorische Voraussetzungen erfüllen. § 11 BDSG regelt die sog. *Auftragsdatenverarbeitung*. Beispiele für die Datenverarbeitung im Auftrag sind der Betrieb eines Rechenzentrums oder eines Callcenters.

Werden dem Auftragnehmer personenbezogene Daten zu diesem Zweck überlassen, findet datenschutzrechtlich gesehen keine Übermittlung statt, da der Auftragnehmer nicht Dritter ist. Gegenüber den Bürgerinnen und Bürgern bleibt der Auftraggeber (also die Stelle, um deren Aufgabe es geht) dafür verantwortlich, dass mit ihren personenbezogenen Daten rechtmäßig umgegangen wird. Dies setzt voraus, dass

- der Auftraggeber einen schriftlichen Auftrag erteilt hat (was genau schriftlich geregelt werden muss, legt § 11 Absatz 2 BDSG detailliert fest),
- der Auftragnehmer nur im Rahmen der Weisungen seines Auftraggebers tätig werden darf und
- der Auftraggeber die erforderlichen Maßnahmen zur Datensicherheit vorgeben muss.

Der Auftraggeber muss sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen und das Ergebnis dieser Überprüfung dokumentieren.

Im Regelfall wird sich der Auftraggeber vor Ort davon vergewissern, dass seine Vorgaben, insbesondere im Hinblick auf die technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes, eingehalten werden. Es ist jedoch möglich, diese Aufgabe gegebenenfalls an vertrauenswürdige Dritte (etwa unabhängige Sachverständige oder Wirtschaftsprüfungsgesellschaften, die kein eigenes Interesse an der Bewertung haben) zu delegieren, die dann die Einhaltung der Vorgaben bescheinigen. Letzteres kommt insbesondere dann in Betracht, wenn die Auftragsdatenverarbeitung im Ausland durchgeführt wird. Werden Aufträge an Auftragnehmer erteilt, die ihren Sitz im Europäischen Wirtschaftsraum haben und die Datenverarbeitung dort ausführen, gelten dieselben Vorgaben wie für inländische Auftragnehmer. Bei der Auftragsvergabe an Auftragnehmer in sonstigen Drittstaaten sind besondere Bedingungen zu beachten, da in diesen Fällen eine Auftragsdatenverarbeitung nach § 11 BDSG nicht möglich ist.

3.4 Werbung und Auskunfteien nach §§ 28 und 29 BDSG

Das BDSG unterscheidet zwischen der Datenerhebung und -verarbeitung für eigene Geschäftszwecke (§ 28 BDSG) und der geschäftsmäßigen Erhebung und Verarbeitung zum Zwecke der Übermittlung (§ 29 BDSG).

Typischerweise handelt es sich im ersteren Fall um ein Unternehmen, das bei seinen eigenen Kundinnen und Kunden im Rahmen der Vertragsbeziehung Daten erhebt und diese zur Erfüllung der Vertragszwecke nutzt. Dies ist ohne ausdrückliche Einwilligung der Betroffenen zulässig. Beispiele: Ein Möbelhändler erhebt bei einem Kunden im Rahmen eines Verkaufs Name und Anschrift, um die Ware liefern zu können. Die Zahlung der Wareerfolgt mit der EC-Karte, der Händler nutzt die so gewonnenen Kontoinformationen ausschließlich zum Zwecke des Bankeinzugs.

Die Tätigkeit von Adresshändlern und Auskunfteien ist hingegen ein Fall der geschäftsmäßigen Datenerhebung und -verarbeitung zum Zwecke der Übermittlung. Geschäftsmäßige Datenverarbeitung liegt vor, wenn im Rahmen einer auf Dauer angelegten Tätigkeit die Datenverarbeitung als solche den Geschäftszweck bildet. Das Gesetz selbst nennt als Beispiele für geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung die Werbung, die Tätigkeit von Auskunfteien oder den Adresshandel. Die Nutzung von personenbezogenen Daten zu Zwecken der postalischen Werbung und des Adresshandels ist abschließend in § 28 Absatz 3 BDSG geregelt. Bestandsdaten im Rahmen von Vertragsverhältnissen mit Telekommunikationsunternehmen dürfen nur im Rahmen des § 95 TKG für Werbung verwendet werden (s. Kapitel 2.5).

Werbung und Adresshandel

Personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung von Betroffenen zu Zwecken der Werbung und des Adresshandels weitergegeben werden. Von diesem Grundsatz gibt es – bezogen auf postalische Direktwerbung – jedoch zahlreiche Ausnahmen.

Ohne Einwilligung dürfen personenbezogene Daten zu Zwecken der Werbung oder des Adresshandels verarbeitet oder genutzt werden,

- wenn für Betroffene anhand der Werbung erkennbar ist, welches Unternehmen seine Adressdaten hierfür weitergegeben hat. Dazu müssen Herkunft und Weitergabe der Adressdaten dokumentiert werden. Bereits aus der Werbung selbst muss für die Betroffenen erkennbar sein, wer die Daten erstmalig weitergegeben hat. Diese Stelle muss den Betroffenen dann auf Nachfrage mitteilen können, an wen sie die Daten zu Werbezwecken in den letzten zwei Jahren übermittelt hat;

- wenn Unternehmen ihre eigenen Kundinnen und Kunden bewerben. Allerdings dürfen sie hierfür nur sog. *Listendaten* nutzen, die sie bei Betroffenen selbst erhoben oder aus allgemein zugänglichen Quellen (etwa Telefonbüchern) entnommen haben. Es dürfen nicht unterschiedslos alle Kundendaten für Werbezwecke herangezogen werden, sondern nur ein gesetzlich bestimmter Datenkatalog: Name, Titel, akademischer Grad, Anschrift und Geburtsjahr, Berufs-, Branchen- oder Geschäftsbezeichnung sowie eine Angabe, die die Zugehörigkeit der Betroffenen zu einer bestimmten Personengruppe charakterisiert (z. B. Versandhauskunde).

Der Zusendung persönlich adressierter Werbung kann man jederzeit widersprechen. Auf dieses Recht muss hingewiesen werden, wenn Werbung zugesandt wird, d. h., es sollte bereits auf dem Werbeschreiben vermerkt sein, wo und wie Widerspruch eingelegt werden kann. Diesen Widerspruch kann man bereits bei der erstmaligen Bekanntgabe seiner persönlichen Daten gegenüber dem Geschäfts- oder Vertragspartner aussprechen, z. B. durch einen entsprechenden Vermerk auf dem Antrags- bzw. Vertragsformular. Der Widerspruch ist aber auch zu einem späteren Zeitpunkt möglich und bedarf keiner weiteren Begründung. Er kann auch bei den Stellen eingelegt werden, denen die Daten übermittelt worden sind.

Personen, die keine Werbung per Briefpost wünschen, können sich in die sog. *Robinsonliste* aufnehmen lassen. Hierzu kann ein Aufnahmeformular unter folgender Anschrift angefordert werden:

DDV-Robinsonliste
Postfach 1454
33244 Gütersloh
Tel.: (05244) 903723

Die Formulare werden auch im Internet als PDF-Datei zum Herunterladen angeboten (https://www.ichhabediewahl.de). Allerdings ist die Nutzung dieser Liste durch die Werbewirtschaft freiwillig, so dass ein Eintrag nicht garantiert, dass man überhaupt keine Werbung mehr erhält.

Ferner gibt die Deutsche Telekom AG die Daten, die auf Wunsch der Kundin oder des Kunden in das Telefonverzeichnis und ggf. in ein elektronisches Verzeichnis (z. B. CD-ROM) aufgenommen werden sollen, an die

DeTeMedien GmbH
Wiesenhüttenstrasse 18
60329 Frankfurt
Tel.: (069) 26 82-0
Fax: (069) 26 82-11 01

weiter. Auch zu einem späteren Zeitpunkt können Kunden gegenüber der Telekom einer Eintragung widersprechen; bei der Neuauflage des Telefonverzeichnisses darf dann die Anschrift nicht mehr enthalten sein.

Auskunfteien

Ein Unternehmen darf unter den Voraussetzungen des § 29 BDSG geschäftsmäßig personenbezogene Daten erheben und verarbeiten, um diese Daten Dritten zu übermitteln. Dies geschieht insbesondere bei Auskunfteien, die anderen Unternehmen Angaben zur Kreditwürdigkeit von Privatpersonen verkaufen. Auskunfteien erheben und speichern Angaben zu vertragsgemäßem wie nicht-vertragsgemäßem Verhalten. § 28a BDSG legt fest, welche personenbezogenen Daten zu nicht-vertragsgemäßem Verhalten bei einer Forderung an Auskunfteien übermittelt und somit von diesen erhoben und verarbeitet werden dürfen.

Folgende personenbezogene Daten dürfen an eine Auskunftei übermittelt werden:

- Forderungen, die durch rechtskräftige Urteile festgestellt worden sind,
- Forderungen im Rahmen von Insolvenzverfahren,
- ausdrücklich anerkannte Forderungen,
- jede Art der Forderung, wenn mindestens zweimal schriftlich gemahnt worden ist, zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen, auf die Übermittlung hingewiesen wurde und die Forderung nicht bestritten worden ist,

- jede Art von Forderung, die den Vertragspartner zur fristlosen Kündigung berechtigt, wenn Betroffene vorher über Übermittlung an eine Auskunftei informiert worden sind.

3.5 Benachrichtigung des Betroffenen nach § 33 BDSG

Nicht-öffentliche Stellen sind verpflichtet, alle Betroffenen individuell zu benachrichtigen, über die sie Daten ohne deren Kenntnis erhoben haben und deren Daten sie speichern oder verarbeiten möchten.

Der Zeitpunkt der Benachrichtigung ist unterschiedlich. Bei Unternehmen, die geschäftsmäßig personenbezogene Daten verarbeiten, muss die Unterrichtung, sofern eine Übermittlung vorgesehen ist, spätestens bei der ersten Übermittlung erfolgen. Alle anderen nicht-öffentlichen Stellen müssen bei der ersten Speicherung benachrichtigen. Die Benachrichtigung muss umfassen:

- die Angabe der verantwortlichen Stelle (Firma, Anschrift),
- die Tatsache, dass erstmals Daten über die Person, die benachrichtigt wird, gespeichert oder übermittelt werden,
- die Art der Daten,
- die Zweckbestimmung der Erhebung bei Verarbeitung oder Nutzung,
- die Empfänger oder Kategorien von Empfängern, soweit Betroffene nicht mit der Übermittlung an diese rechnen müssen.

In bestimmten, im Gesetz genannten Fällen, erfolgt keine Benachrichtigung, etwa weil eine überwiegende Geheimhaltungspflicht besteht, die Unterrichtung einen unverhältnismäßigen Aufwand erfordert oder Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt haben (s. hierzu im Einzelnen §§ 19a Absatz 2, 33 Absatz 2 BDSG).

3.6 Auskunftsanspruch des Betroffenen nach § 34 BDSG

Das Datenschutzrecht stellt denjenigen, deren personenbezogene Daten durch Dritte erhoben, verarbeitet oder genutzt werden, Instrumente zur Verfügung, um ihr Recht auf informationelle Selbstbestimmung wahrzunehmen. § 34 BDSG regelt das Auskunftsrecht von Betroffenen, damit diese prüfen können, ob die für die Datenverarbeitung verantwortliche Stelle rechtmäßig handelt. Jeder – unabhängig von Alter, Wohnsitz und Nationalität – hat das Recht auf Auskunft über die zur eigenen Person gespeicherten Daten. Das TKG selbst enthält keine spezielle Vorschrift zum Auskunftsrecht, so dass hier das BDSG gilt.

Welche Auskunft kann verlangt werden?

Jeder kann über die zu seiner Person gespeicherten Daten Auskunft verlangen, einschließlich der Angabe, woher sie stammen und an wen sie weitergegeben werden. § 34 BDSG spricht hier von Empfängern oder Kategorien von Empfängern. Der Begriff des Empfängers umfasst nicht nur Dritte außerhalb der verantwortlichen Stelle, sondern auch natürliche Personen oder Stellen, die im Geltungsbereich des BDSG für einen anderen im Auftrag Daten verarbeiten, sowie auch verschiedene Organisationseinheiten innerhalb einer Stelle. Auch die Information über die Kategorien der Empfänger kann für den Einzelnen von erheblicher Bedeutung sein. So macht es z. B. einen Unterschied, ob es sich bei den Empfängern um natürliche Personen handelt oder um bestimmte Branchen oder Unternehmen wie z. B. Auskunfteien oder andere geschäftsmäßige Datenverarbeiter etc.. Darüber hinaus kann man Auskunft über den Zweck der Speicherung erhalten, d. h. die betreffende Verwaltungsaufgabe oder den speziellen Geschäftszweck.

Von Kreditauskunfteien und anderen Stellen, die geschäftsmäßig Daten zum Zweck der Übermittlung speichern, kann Auskunft auch über Daten verlangt werden, die weder in einer automatisierten Verarbeitung noch in einer nicht-automatisierten Datei gespeichert sind (z. B. ungeordnete Akten oder Hefter). Diese Stellen müssen auch sagen, woher sie die Daten haben und an wen sie die Daten weitergeben, es sei denn, die Stelle könnte geltend machen, dass ihr Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Auskunftsinteresse überwiegt. Von allen Stellen, die Scorewerte einsetzen oder errechnen, hat man das Recht zu erfahren, welche Scorewerte zur Per-

son gespeichert, an Dritte übermittelt worden und wie diese Scorewerte zustande gekommen sind. Der Scorewert muss verständlich, einzelfallbezogen und nachvollziehbar erklärt werden. Wenn jemand seinen Auskunftsanspruch geltend macht, darf sich dies nicht negativ auf den Scorewert auswirken.

Wie erhält man Auskunft?

Es empfiehlt sich, die Auskunft schriftlich anzufordern. Zur Legitimation genügt es in der Regel, die Kopie eines Personaldokuments beizulegen. Einschreiben ist nicht erforderlich. Bei persönlicher Vorsprache wird eine sofortige Erledigung oft nicht möglich sein. Wenn man anruft, kann man meist nicht sicher identifiziert werden, so dass der Grundsatz gilt: Keine telefonische Datenauskunft. Besser schreibt man möglichst genau, worüber die Auskunft gewünscht wird (also z. B. „meine Daten im Zusammenhang mit meinem Festnetzanschluss“, aber nicht „alles, was das Unternehmen über mich hat“).

Was kostet eine Auskunft?

Grundsätzlich muss für die Auskunft nichts bezahlt werden. Von Auskunfteien und anderen Stellen, die Daten geschäftsmäßig zum Zwecke der Übermittlung speichern, hat jeder das Recht, einmal im Kalenderjahr kostenlos Auskunft zu erhalten. Für jede weitere Auskunft kann jedoch ein Entgelt verlangt werden, wenn die Auskunft gegenüber Dritten wirtschaftlich genutzt werden kann (etwa um die Bonität nachzuweisen). Das geforderte Entgelt darf nicht höher sein als die entstandenen direkt zurechenbaren Kosten. Aber auch bei derartigen Auskünften muss nichts bezahlt werden, wenn besondere Umstände dafür sprechen, dass Daten unrichtig oder unzulässig gespeichert sind oder sich dies aus der Auskunft ergibt. Bei einer mündlichen Auskunft oder einer Auskunft auf einem Blatt ohne Namensangabe entstehen keine Kosten. Auf die Möglichkeit, durch persönliche Kenntnisnahme die Auskunft unentgeltlich zu erhalten, muss die speichernde Stelle ausdrücklich hinweisen. Gegebenenfalls können Auskünfte auch elektronisch, etwa per E-Mail, erteilt werden. Dabei ist allerdings zu beachten, dass mit der elektronischen Übermittlung gegebenenfalls zusätzliche Risiken verbunden sein können, insbesondere, wenn keine verschlüsselte Datenübermittlung gewährleistet ist.

Was tun, wenn die Auskunft verweigert wird?

Jeder hat grundsätzlich einen Anspruch auf eine vollständige Auskunft. *Nicht-öffentliche Stellen* dürfen eine Auskunft nur in Fällen ablehnen, in denen auch keine Benachrichtigungspflicht besteht (s. hierzu im Einzelnen §§ 34 Absatz 7 i. V. m. 33 Absatz 2 Satz 1 Nr. 2, 3 und 5 bis 7 BDSG).

Soweit die auskunftspflichtige Stelle nicht oder und nur teilweise Auskunft erteilt, muss sie auf die Unvollständigkeit der Auskunft ausdrücklich hinweisen, damit man die Möglichkeit erhält, eine Überprüfung zu verlangen. Im Allgemeinen ist die verantwortliche Stelle auch verpflichtet zu begründen, aufgrund welcher gesetzlichen Bestimmung und aufgrund welcher Tatsachen sie eine Auskunft verweigert oder beschränkt. Eine solche Begründung ist nur entbehrlich, wenn sonst der mit der Auskunftsverweigerung verfolgte Zweck (z. B. laufende polizeiliche Ermittlungen nicht zu behindern) gefährdet würde. Bestehen Zweifel, ob eine korrekte Auskunft erteilt worden ist, kann man sich an die zuständige Datenschutzaufsichtsbehörde wenden oder eine Klage bei Gericht einlegen.

3.7 Auskunftsansprüche nach § 101 Urheberrechtsgesetz

Heute werden Musik- oder Filmdateien oft illegal verbreitet. Gegen diese Art der Urheberrechtsverletzung geht die Musik- und Filmindustrie als Rechteinhaber vor. Sobald eine nutzende Person eine Datei, die in einem Peer-to-Peer-Netzwerk angeboten wird, auf den eigenen PC heruntergeladen hat, wird diese Datei häufig automatisch auf dem Computer dieses Nutzers zum Download für andere angeboten. Das Anbieten einer urheberrechtlich geschützten Datei stellt einen Verstoß gegen § 19a UrhG dar.

Auskunftsanspruch des Rechteinhabers

Zur Verfolgung dieses Verstoßes hat der Gesetzgeber den Rechteinhabern in § 101 Absatz 9 UrhG das Recht eingeräumt, Auskunft über die Identität des Rechteverletzers zu erhalten. Um diesen Auskunftsanspruch verwirklichen zu können, wird die IP-Adresse des Rechteverletzers samt Datum und Uhrzeit benötigt. Die Rechteinhaber bedienen sich bestimmter Dienstleister, die mit Hilfe einer Software und anhand von sog. Signaturen die zum Download angebotenen eigenen Dateien erkennen und die IP-Adresse des

anbietenden PCs zusammen mit Datum und Uhrzeit speichern. Der Rechteinhaber stellt dann unter Angabe der so gesammelten Daten (IP-Adresse, Datum, Uhrzeit) bei dem zuständigen Landgericht einen Antrag, dem jeweiligen Internet-Zugangsprovider die Auskunftserteilung unter Verwendung der Verkehrsdaten zu gestatten (sog. *Antrag auf Gestattung).* Für die Auskunftserteilung ist eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten erforderlich, da bei der Ermittlung der Identität des Rechteverletzers das Fernmeldegeheimnis betroffen ist (§ 101 Absatz 9 UrhG).

Die betreffenden Verkehrsdaten dürfen vom Internet-Zugangsprovider jedoch nur im Rahmen der gesetzlichen Bestimmungen für sehr begrenzte Fristen gespeichert werden, so dass Gerichte dazu übergegangen sind, unmittelbar nach Antragstellung des Rechteinhabers durch eine einstweilige Anordnung ein fristgemäßes Löschen der Verkehrsdaten zu verhindern. Mit dem sog. *Sicherungsbeschluss* wird der Internet-Zugangsprovider dabei zunächst verpflichtet, die betreffenden Verkehrsdaten aufzubewahren. Stellt das Gericht fest, dass die Voraussetzungen des Auskunftsanspruches aus § 101 Absatz 9 UrhG vorliegen, und somit die Verwendung der Verkehrsdaten zulässig ist, ergeht der sog. *Gestattungsbeschluss.* Erst dieser Beschluss führt zu einer Herausgabe des Namens und der Adresse durch den Internet-Zugangsprovider an den Rechteinhaber bzw. an die ihn vertretende Anwaltskanzlei.

Ist ein sog. *Reseller* (ein Service-Provider, der die Vermittlung des Internet-Zugangs als eigene Dienstleistung anbietet und sich dabei der technischen Einrichtung eines Netzbetreibers bedient; er verfügt über die zur Identifikation notwendigen Bestandsdaten seiner Kundinnen und Kunden, während der Netzbetreiber die IP-Adressen vergibt und dabei nur die Benutzerkennungen erfährt) im Spiel, so läuft das Verfahren zweistufig ab: Der Netzbetreiber beauskunftet im ersten Schritt, welcher Benutzerkennung bei welchem Reseller eine bestimmte IP-Adresse zugewiesen war. Danach muss der Reseller dem Rechteinhaber mitteilen, wer der Inhaber der Benutzerkennung ist. Hierbei handelt es sich um eine Bestandsdatenauskunft nach § 101 Abs. 2 Nr. 3 UrhG, für die kein richterlicher Beschluss erforderlich ist. Der Rechteinhaber kann dann die zivilrechtlichen Schritte gemäß §§ 97, 97a UrhG (Abmahnung, Aufforderung zur Abgabe einer Unterlassungserklärung und zur Zahlung von Schadensersatz) gegen den ermittelten Rechteverletzer einleiten.

Auskunftsanspruch des angeblichen Rechteverletzers

Wer erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis der Betroffenen speichert, muss gemäß § 33 Abs. 1 BDSG Betroffene über die Speicherung, die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle benachrichtigen. Sobald der Rechteinhaber die Daten der Internet-Zugangsprovider erstmalig erhält, muss er also die Betroffenen hierüber informieren. Seiner Benachrichtigungspflicht kommt der Rechteinhaber regelmäßig in Form von Abmahnungen nach.

Eine konkrete Auskunft des Internet-Zugangsproviders, welche Daten weitergegeben wurden, kann unter Berufung auf § 34 Abs. 1 Nr. 2 BDSG nicht eingefordert werden. Denn diese Vorschrift kennt keine Verpflichtung zur Auskunftserteilung über Daten, die weitergegeben wurden, sondern lediglich über den Empfänger oder Kategorien von Empfängern. Tatsächlich wäre der Internet-Zugangsprovider gar nicht in der Lage, eine solche Auskunft zu erteilen, da er die betreffenden Verkehrsdaten nach Abschluss des Auskunftsverfahrens löschen muss. Welche IP-Adresse dem Beschuldigten zu einem bestimmten Zeitpunkt zugeordnet war, kann der Internet-Zugangsprovider folglich im Regelfall nicht mehr beauskunften.

3.8 Auskünfte an Strafverfolgungsbehörden nach §§ 100g und 100j StPO

Jeder Diensteanbieter ist zur Wahrung des Fernmeldegeheimnisses verpflichtet. Eingriffe in das Fernmeldegeheimnis sind nur dann zulässig, wenn sie gesetzlich angeordnet sind. Die StPO enthält Rechtsgrundlagen für Strafverfolgungsbehörden, aufgrund derer die Telekommunikationsdiensteanbieter die Überwachung der Telekommunikation zu ermöglichen haben (§§ 100a und 100b StPO) oder Auskünfte z. B. über die Bestandsdaten (§ 100j StPO) und die Verkehrsdaten (§ 100g StPO) erteilen müssen. Das TKG selbst enthält keine gesonderte Speichererlaubnis für Zwecke der Strafverfolgung. Für eine Auskunftserteilung auf Ersuchen von Sicherheitsbehörden mit Aufgaben im Bereich der Strafverfolgung dürfen ausschließlich Daten verwendet werden, die bei den Telekommunikationsdiensteanbietern rechtmäßig gespeichert sind.

Auskunftsersuchen nach § 100g StPO

Nach § 100g Absatz 1 Satz 1 StPO dürfen zur Verfolgung bestimmter Straftaten von auch im Einzelfall erheblicher Bedeutung oder wenn eine Straftat mittels Telekommunikation begangen wird, ohne Wissen von Betroffenen Verkehrsdaten nach § 96 Absatz 1 TKG erhoben werden. Diese Daten müssen für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich sein. Wurde eine Straftat mittels Telekommunikation begangen, ist diese Maßnahme nur zulässig, wenn die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist bei diesen Straftaten nicht zulässig (§ 100g Absatz 1 Satz 3 StPO). Das Auskunftsersuchen ist grundsätzlich an das Vorliegen einer richterlichen Anordnung nach § 100b StPO gebunden. Die Vorschrift des § 100g StPO ist eine der in § 96 Absatz 1 Satz 2 TKG erwähnten „anderen gesetzlichen Vorschriften“ und begründet eine Auskunftspflicht des Diensteanbieters (s. Kapitel 2.6).

Auskunftsersuchen nach § 100j StPO

Die Vorschrift des § 100j StPO ist erst am 1. Juli 2013 in Kraft getreten und Konsequenz der Entscheidung des BVerfG vom 24. Januar 2012, in der es um die Verfassungsmäßigkeit der Regelungen zur Verpflichtung geschäftsmäßiger Anbieter von Telekommunikationsdiensten ging, bestimmte Bestandsdaten zu speichern und diese im Wege des automatisierten oder manuellen Auskunftsverfahrens gemäß §§ 112 und 113 TKG zu beauskunften (s. Kapitel 2.20 und 2.21). Wie das BVerfG entschieden hat, bedarf es für den Abruf von Bestandsdaten grundsätzlich qualifizierter Rechtsgrundlagen, die eine Auskunftspflicht der Diensteanbieter selbst normenklar begründen. Dieses auch *Doppeltürenmodell* genannte Prinzip wurde vom BVerfG damit begründet, dass sich ein Datenaustausch immer durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung vollzieht, die jeweils einer eigenen Rechtsgrundlage bedürfen.

§ 100j StPO ermächtigt Strafverfolgungsbehörden, die nach den §§ 95 (s. Kapitel 2.5) und 111 (s. Kapitel 2.19) TKG gespeicherten Bestandsdaten (wie z.B. Name und Anschrift des Anschlussinhabers, zugeteilte Rufnummern und andere Anschlusskennungen) bei Diensteanbietern abzufragen, soweit dies für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Hierunter fallen

auch die ausdrücklich hervorgehobenen Zugangssicherungscodes, also Daten, durch die der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, und die Zuordnung von zu einem bestimmten Zeitpunkt zugewiesenen IP-Adressen zu einem konkret Teilnehmenden.
Bei Zugangssicherungscodes schränkt das Gesetz die Abfragemöglichkeit zudem dahingehend ein, dass bereits vor der Abfrage die Voraussetzungen für die spätere Nutzung der Daten vorliegen. Darüber hinaus ist nach § 100j Absatz 3 StPO grundsätzlich eine richterliche Anordnung erforderlich. Schließlich ist in Absatz 4 der Norm eine Benachrichtigungspflicht der von der Auskunft betroffenen Personen vorgesehen, sofern es sich bei dem Auskunftsbegehren um Zugangssicherungscodes oder die Zuordnung von IP-Adressen gehandelt hat.

3.9 Telemediengesetz

Das Telemediengesetz (TMG) ist in fünf Abschnitte gegliedert. Die Abschnitte 1 bis 3 gelten nicht nur für Anbieter von Telemedien, sondern auch für Internet-Zugangsprovider und Anbieter von E-Mail-Diensten. Dieser auf den ersten Blick überraschende Systembruch wird in der Gesetzesbegründung erläutert, wonach diese Angebote neben der Übertragungsdienstleistung auch eine inhaltliche Dienstleistung anbieten und insoweit die Anwendbarkeit des TMG gegeben ist.

Anwendungsbereich und Informationspflichten

Abschnitt 1 regelt u. a. den Anwendungsbereich und das Herkunftslandprinzip, *Abschnitt 2* enthält neben der Bestimmung zur Zulassungsfreiheit besondere Regelungen zu den Informationen, die der Diensteanbieter in einem *Impressum* auf seiner Website veröffentlichen muss (§ 5 TMG). Dies sind zumindest der Name, die Anschrift und Angaben zur unmittelbaren und elektronischen Kontaktaufnahme. Unter bestimmten Voraussetzungen sind weitere Angaben erforderlich: z. B. bei juristischen Personen der Vertretungsberechtigte, ggf. Angaben zum Handelsregister oder die Umsatzsteueridentifikationsnummer. Diese Informationen sind aus Verbrauchersicht von besonderer Bedeutung, da sie den Bürgerinnen und Bürgern die Möglichkeit geben, z. B. bei Verstößen gegen den Datenschutz ihre Rechte wahrzunehmen. Die Impressumspflicht gilt jedoch nur für solche Angebote, die in der Regel gegen Entgelt angeboten werden. An-

gebote mit rein privatem Charakter, z. B. private Websites/Homepages oder solche von Idealvereinen, sind von dieser Verpflichtung ausgenommen.

Besondere Vorschriften gilt es bei kommerziellen Internet-Angeboten und beim Versand von Werbe-E-Mails zu beachten, die alle dem Transparenzgebot folgen und damit Nutzende vor Abzocke und Betrug schützen sollen und das Problem der unerwünschten E-Mails zumindest verringern wollen (§ 6 TMG). Die wesentlichen Regelungen sind: Die verantwortliche natürliche oder juristische Person muss identifizierbar sein, Teilnahmebedingungen müssen leicht zugänglich und unzweideutig angegeben sein, bei Werbe-E-Mails dürfen weder der Absender noch der kommerzielle Charakter verheimlicht oder verschleiert werden. Der Versand von massenhaften Spam-Mails, teils mit schädlichen Inhalten, fällt nicht unter diese Regelung und muss an anderer Stelle und mit starken und wirksamen technischen Mitteln gestoppt werden (s. Kapitel 4.5).

Verantwortlichkeit der Diensteanbieter

Abschnitt 3 enthält Regelungen zur Verantwortlichkeit der Diensteanbieter. Hier wird verständlich, warum der Regelungsbereich des TMG in Teilen auch Internet-Zugangsprovider und Anbieter von E-Mail-Diensten umfasst. Grundsätzlich ist jeder Anbieter für die eigenen Inhalte verantwortlich, die er den Nutzenden zur Verfügung stellt. Anders sieht es aus, wenn es sich um fremde Inhalte handelt oder um solche, die nur durchgeleitet oder zur beschleunigten Übermittlung zwischengespeichert werden: In diesen Fällen ist der Diensteanbieter grundsätzlich von der Haftung befreit. Allerdings muss er immer dann, wenn ihm rechtswidrige Handlungen oder Informationen gemeldet werden, handeln und die betreffenden Inhalte entfernen. Im Umkehrschluss ist der Anbieter nicht verpflichtet, den Internet-Verkehr, der über seine Server läuft, zu überwachen.

Datenschutzprinzipien für Telemedienangebote

Die Datenschutzprinzipien *Verbot mit Erlaubnisvorbehalt* und *Zweckbindung* stehen am Anfang des *Abschnitts 4,* der den Datenschutz für Telemedienangebote regelt. Insbesondere wird in § 12 Absatz 1 klargestellt, dass die Erlaubnistatbestände im TMG abschließend geregelt sind; eine Rechtsvorschrift in einem anderen Gesetz kann nur dann subsidiär herangezogen werden, wenn diese sich ausdrücklich auf Telemedien bezieht.

Zu den wesentlichen Pflichten des Diensteanbieters gehört die Informationspflicht gegenüber denjenigen, die das Angebot in Anspruch nehmen, d. h. der Anbieter muss darlegen, welche personenbezogenen Daten und zu welchem Zweck er erhebt und ggf. verwendet. Inhaltlich muss hier zwischen den Bestands- und Nutzungsdaten (§§ 14 und 15 TMG) unterschieden werden: Bestandsdaten sind z. B. Nutzername und Passwort, die den Zugang zu einem Angebot ermöglichen, Nutzungsdaten z. B. IP-Adresse, Datum, Uhrzeit, aufgerufene Seite, die beim Besuch einer Website immer und auch ohne Anmeldung anfallen. Viele personenbezogene Daten, die Nutzende bei Telemedienangeboten wie z. B. in einem sozialen Netzwerk oder in einem Bestellformular (die Lieferadresse) einstellen, können weder als Bestands- noch als Nutzungsdaten im Sinne des TMG qualifiziert werden. Es handelt sich um darüber hinausgehende sog. Inhaltsdaten, deren Verarbeitung sich nach dem BDSG richtet.

Die Pflicht, die Nutzung von Telemedien anonym oder unter Pseudonym zu ermöglichen, besteht, soweit dies technisch möglich und zumutbar ist (§ 13 Absatz 6 TMG). Will der Anbieter die Einwilligung von Nutzenden elektronisch einholen, so ist er verpflichtet, bestimmte Bedingungen zu erfüllen (§ 13 Absatz 2 TMG). Das TMG enthält hierzu konkrete Regelungen, insbesondere die Forderung nach einer bewussten und eindeutigen Handlung der nutzenden Person, die inzwischen auch in das TKG aufgenommen worden sind.

Die Erhebung und Verwendung von Bestands- und Nutzungsdaten ist nach dem TMG auf Zwecke des Vertragsverhältnisses bzw. der Diensterbringung und -abrechnung beschränkt. Nach den Urteilen des Europäischen Gerichtshofes vom 19. Oktober 2016 (C-582/14) und des Bundesgerichtshofes vom 16. Mai 2017 (VI ZR 135/13) ist § 15 TMG (Nutzungsdaten) entsprechend Artikel 7 Buchstabe f der Richtlinie 95/46/EG, in der Auslegung des EuGH, dahingehend anzuwenden, dass ein Online-Mediendiensteanbieter personenbezogene Daten von Nutzern dieser Dienste ohne deren Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus erheben und verwenden darf, soweit ihre Erhebung und Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten. Unabdingbar ist jedoch eine Abwägung mit dem Nutzerinteresse und dessen Grundrechten und Grundfreiheiten. Des Weiteren ist ausdrücklich die Erstellung von Nutzungsprofilen bei Verwendung von Pseudonymen erlaubt (§ 15

Absatz 3 TMG). Nutzende haben jedoch auch hier ein Widerspruchsrecht, auf das sie hingewiesen werden müssen. Allerdings wird bei der in der Praxis vielfach heimlichen Profilbildung diese Vorgabe missachtet.

Eine Auskunftsverpflichtung der Anbieter von Telemedien ergibt sich aus § 14 Absatz 2-5 TMG für Bestandsdaten und aus § 15 Absatz 5 Satz 4 i.V. m. § 14 Absatz 2-5 TMG für Nutzungsdaten. Eine eigene Regelung zur Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten enthält das TMG nicht, § 15a TMG verweist hierzu auf § 42a BDSG (s. Kapitel 2.17).

Bußgeldvorschriften

Im *Abschnitt 5* finden sich in § 16 TMG die Bußgeldvorschriften, wonach eine Ordnungswidrigkeit mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden kann (§ 16 Absatz 3 TMG). Allerdings enthält das TMG keine Regelung über die zuständige Verwaltungsbehörde, so dass die allgemeinen Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) gelten; nach § 36 Absatz 1 OWiG ist für die Verfolgung von Ordnungswidrigkeiten die Behörde sachlich zuständig, die durch Gesetz bestimmt wird bzw. mangels einer solchen die fachlich zuständige oberste Landesbehörde. In den einzelnen Bundesländern gibt es hierzu unterschiedliche Regelungen.

Anders als im TKG findet sich im TMG auch keine Regelung zur Zuständigkeit der Datenschutzaufsicht (s. Kapitel 2.22). Insofern gilt die Vorgabe des BDSG, so dass sich die Zuständigkeit der Aufsichtsbehörden nach der jeweiligen verantwortlichen Stelle richtet. Im nicht-öffentlichen Bereich sind demnach grundsätzlich die Datenschutzaufsichtsbehörden der Länder zuständig.

Problematisch wird die Bestimmung der zuständigen Aufsichtsbehörde allerdings dann, wenn ausländische Diensteanbieter wie z. B. Facebook oder Google ihre Datenverarbeitung außerhalb von Deutschland abwickeln und zudem auch keinen innerdeutschen Firmensitz haben. Ob auch in diesen Fällen trotzdem die Zuständigkeit einer deutschen Datenschutzaufsichtsbehörde gegeben sein kann, ist ungeklärt. Viele dieser Unternehmen sehen sich jedenfalls als nicht dem deutschen Datenschutzrecht unterworfen an, so dass in der Praxis die Aufsichtsbehörde des Landes kontaktiert werden muss, in dem das Unternehmen seinen Firmensitz hat.

4 Weitere praktische Datenschutzfragen

4.1 Telekommunikationsanlagen von Firmen und Behörden

Als Telekommunikations- oder auch Nebenstellenanlage (TK-Anlage) bezeichnet man eine Vermittlungseinrichtung, die es gestattet, mehrere Telefone (und auch andere Geräte wie z. B. Fax) direkt untereinander oder mittels einer oder mehrerer Leitungen mit einem öffentlichen Telefonnetz („Amtsanschlüsse“) zu verbinden und zu betreiben. Wesentliches Merkmal einer Telefonanlage ist die Möglichkeit der (meist kostenfreien) internen Telefonie innerhalb dieser Anlage. Bei externen Gesprächen in ein öffentliches Telefonnetz teilen sich die an der Anlage betriebenen Endgeräte die zur Verfügung stehenden Zuleitungen zu öffentlichen Telekommunikationsnetzen, da nicht einzelne Teilnehmende einen separaten Zugang benötigen. Weiterhin bietet eine Telefonanlage diverse nützliche Leistungsmerkmale wie z. B. das Weiterverbinden von Anrufen, die Bereitstellung von Sammelrufnummern oder auch Rufum- und Rufweiterleitungen. Waren bis vor einigen Jahren überwiegend ISDN-basierte TK-Anlagen in Betrieb, sind heute überwiegend VoIP-Anlagen üblich (s. Kapitel 4.1.3). Im Zuge der technischen Fortentwicklung werden neben „schnurlosen Telefonen“ nach dem DECT-Standard (s. Kapitel 4.2.1) auch mobile WLAN-Telefone an TK-Anlagen verwendet.

Nachfolgend werden die beim Betrieb von Telekommunikationsanlagen datenschutzrechtlich relevanten Themen erläutert sowie Hinweise gegeben, wie der Betrieb datenschutzkonform gestaltet werden kann; ergänzend sei auf den IT-Grundschutz-Katalog des BSI hingewiesen, der auf dessen Website (www.bsi.bund.de) veröffentlicht ist.

4.1.1 Unified Communications

Tatsächlich hat sich im deutschen Sprachgebrauch für diesen Anglizismus noch keine einheitliche Bezeichnung gefunden, die den vollen Umfang der Technologie abbilden könnte. *Unified Communications* oder kurz UC (englisch für „vereinheitlichte Kommunikation“) beschreibt die Integration von unterschiedlichen Kommunikationsmedien in einer einheitlichen Anwendungsumgebung. Die grundsätzliche Idee hinter diesem Ansatz ist, Erreichbarkeiten zu verbessern und Geschäftsprozesse effizienter zu gestalten. Im praktischen Beispiel findet man so sehr häufig die Integration der Telefoniedienste moderner TK-Anlagen innerhalb des ohnehin ständig auf dem PC präsenten E-Mail-Programms, garniert mit einem Instant Messenger, der den Kolleginnen und Kollegen anhand einer Statusnachricht Auskunft darüber gibt, ob der jeweilige Mitarbeiter gerade in einem Meeting ist oder für ein Gespräch zu Verfügung steht. Diese Symbiose birgt auch einige datenschutzrechtliche Fallstricke, die es zu beachten gilt.

Medienintegration

Die Medienintegration ist sehr unterschiedlich und es gibt nur wenige Gemeinsamkeiten, da auch die Hersteller von TK-Anlagen und UC-Software nicht immer gleich sind. Beim Einsatz einer solchen UC-Lösung sollte auf folgendes geachtet werden:

Da sehr häufig die Telefonie als Komfortfunktion integriert ist, weisen die UC-Anwendungen Programmbestandteile auf, die sonst den Leistungsmerkmalen (s. Kapitel 4.1.2) zugeordnet werden. Diese werden allerdings gänzlich unabhängig von den Vorgaben und Einstellungen der TK-Anlage umgesetzt. In den meisten Fällen sind in UC- Anwendungen vorgehaltene Anruflisten nicht mit einer Löschfrist belegt, was zu einer Speicherung von Rufnummern über den angemessenen Rahmen hinaus führt. Durch die gegebene Heterogenität beschränkt sich dieses Phänomen leider nicht nur auf die Sprachtelefonie, sondern lässt sich auch für geführte Videotelefonate und Chats beobachten. Die Speicherpraxis solcher Anwendungen sollte nicht nur Anwendenden überlassen werden, sondern von vornherein durch den Administrator auf einen angemessenen Rahmen festgelegt werden; eine zusätzliche Löschmöglichkeit für Rufnummernhistorien etc. durch die Nutzerinnen und Nutzer selbst erscheint sinnvoll.

Präsenzinformation

Die meist nahtlose Integration der unterschiedlichen Medien- und Informationsquellen ermöglicht auch Ungeahntes, wenn es um die Frage geht, ob ein einzelner Mitarbeiter oder gar eine ganze Gruppe zu einem bestimmten Zeitpunkt verfügbar ist oder nicht. Die sog. *Präsenzinformation* stellen die meisten Programme ganz freizügig unternehmensweit zur Verfügung. Diese Funktion erleichtert die Planung von Besprechungen und gemeinsamen Terminen. Oft weiß der einzelne Beschäftigte gar nicht, dass die in dem persönlichen Kalender eingepflegten Termine zur Preisgabe der Präsenzinformationen genutzt werden, da die Anwendungen (besonders, wenn alle aus der Hand eines Herstellers sind) so stark verschmolzen sind, dass eine Interaktion nicht mehr erkennbar ist. Hier ist eine Sensibilisierung jedes Einzelnen gefragt, der darauf achten muss, private Termine auch wirklich als privat zu kennzeichnen.

Zudem sollten Präsenzinformationen nur dann eingesetzt werden, wenn es tatsächlich notwendig ist, denn eine flächendeckende Verhaltenskontrolle sollte vermieden werden. Die zu manchen modernen Kommunikationssystemen gratis vom Hersteller gereichten Universial Serial Bus (USB) -Gadgets, die – fröhlich tanzend – auf dem Bildschirm sitzend mit rotem und grünem Licht dem Großraumbüro anzeigen, dass die betreffende Person gerade „beschäftigt“ ist, sind nicht immer hilfreich.

4.1.2 Leistungsmerkmale

Leistungsmerkmale oder auch *Dienstmerkmale* moderner Telekommunikationsanlagen beschreiben die Funktionalitäten, die von dem Telekommunikationsdienst unterstützt werden. Ein Telekommunikationsdienst lässt sich grundsätzlich durch die Gesamtheit seiner Leistungsmerkmale technisch vollständig beschreiben. Dienst- oder Leistungsmerkmale können formal in drei Gruppen unterteilt werden:

- Zu den *allgemeinen Anschlussmerkmalen* zählen z. B. die Anzahl der verwendeten Kanäle, die Übertragungsrate und die Art der Vermittlungstechnik,
- *Basisdienstmerkmale* umfassen die Beschreibung der Informationsübertragung, wie z. B. den Verbindungsauf- und -abbau sowie die genutzten Protokoll- und Zeichensätze,

- die *ergänzenden Dienstmerkmale* umfassen zusätzlich durch das Netz zur Verfügung gestellte, teilnehmerbezogene Dienste wie z. B. die Übertragung der Rufnummer oder die Möglichkeit zur Durchführung von Konferenzschaltungen.

Prinzipiell betrachtet sind Leistungsmerkmale zunächst unabhängig vom zugrundeliegenden Kommunikationssystem, in der Praxis unterscheidet sich die Ausprägung jedoch stark zwischen den am Markt befindlichen Telekommunikationsanlagen. Bei aktuellen Telekommunikationsanlagen können gezielt Leistungsmerkmale für einzelne Nebenstellen freigegeben oder aber auch gezielt gesperrt werden.

Das Gefährdungspotenzial moderner Telekommunikationsanlagen steigt mit ihrer jeweiligen Komplexität und zunehmenden Funktionalität. Beispielhaft seien das Aufschalten auf bestehende Verbindungen, der unbemerkte Aufbau einer Dreierkonferenz, die Rufumleitung auf einen Fremdapparat oder das direkte Ansprechen einer Teilnehmerin bzw. eines Teilnehmers (Wechselsprechanlage) genannt. Diese oder ähnliche Leistungsmerkmale können – vorausgesetzt, entsprechendes Fachwissen ist vorhanden – zum Gebührenbetrug oder Abhören missbraucht werden.

Die Verhinderung des Missbrauchs von nützlichen Funktionalitäten bedarf einer Reihe von Maßnahmen, die gewährleisten, dass die in vielen Telekommunikationsanlagen vorhandenen Sicherheitsmechanismen auch genutzt werden. Von besonderer Bedeutung sind hierbei die ordnungsgemäße Konfiguration der Anlage und, je nach verwendeter Technologie, auch die Konfiguration der notwendigen Netzwerktechnik. Im Rahmen der technisch-organisatorischen Maßnahmen ist u.a. auch sicherzustellen, dass ausschließlich befugtes Personal Zugriff auf die Anlage und die zugehörigen Systemkomponeten hat. In solche Überlegungen ist auch die Zugriffsmöglichkeit per Fernwartung mit einzubeziehen. In diesem Zusammenhang ist auf den Katalog von Sicherheitsanforderungen (s. Kapitel 2.16) sowie die vom BSI herausgegebene Publikation „*Technische Leitlinie Sichere TK-Anlagen*“ zu verweisen, die Hinweise zum sicheren Betrieb und (insbesondere für Behörden) zur Beschaffung von Telekommunikationsanlagen enthalten (s. www.bsi.bund.de). Nicht benötigte Leistungsmerkmale sollten grundsätzlich deaktiviert werden. Manche Telekommunikationsanlagen verfügen über Ländereinstellungen, bei denen auch rechtliche Vorgaben für die verschiedenen Län-

der berücksichtigt sind. Es sollte darauf geachtet werden, in jedem Fall auch „*Deutschland*“ zu aktivieren.

Anruflisten

Moderne Telefongeräte („Komfort-Telefone“) verfügen meist über die Möglichkeit, sog. *Anruflisten* abzurufen. Dabei können – abhängig von der verwendeten Anlage – z. B. die folgenden Informationen abgerufen werden:

- Anrufe in Abwesenheit
- Angenommene Anrufe
- Abgegangene Telefongespräche

Je nach eingesetzter Telefonanlage können in diesen Anruflisten neben den entsprechenden Telefonnummern auch Datum und Uhrzeit abrufbar sein. Aus Sicht der Nutzenden stellen diese Listen ein sinnvolles Leistungsmerkmal dar, können ihnen doch die in Abwesenheit eingegangenen Anrufe entnommen und die entsprechenden Personen durch Anwahl der Rufnummer aus der Liste zurückgerufen werden. Ebenso komfortabel lassen sich die Rufnummern aus der Liste der abgegangenen Gespräche auswählen, um häufig frequentierte Gesprächspartner zu kontaktieren. Trotz des hier beispielhaft aufgeführten Komforts ist dies aus datenschutzrechtlicher Sicht eher kritisch zu sehen, vor allem, wenn die Telefonanlage im beruflichen Umfeld genutzt wird. Die in den Anruflisten gespeicherten Informationen stellen Verkehrsdaten gemäß § 96 TKG dar (s. Kapitel 2.6). Ist das Leistungsmerkmal *Anruflisten* verfügbar, so ist die Speicherung der Telefonnummern generell auf einen angemessenen Rahmen zeitlich zu begrenzen. Dies sollte durch entsprechende Konfiguration der TK-Anlage erfolgen und nicht den einzelnen Nutzenden durch Einstellungen am Telefongerät (soweit dies technisch möglich ist) überlassen werden. Anruflisten, die nicht wirklich vom Telefonnutzer benötigt werden (Beispiel: angenommene Anrufe), sollten durch entsprechende Konfiguration vom TK-Anlagen-Betreiber überhaupt nicht zur Verfügung gestellt und so eine nicht notwendige Datenspeicherung vermieden werden.

Ergänzend zu diesen technischen Maßnahmen wird den Betreibern von TK-Anlagen empfohlen, alle Nutzerinnen und Nutzer der Anlage in regelmäßigen Abständen über diese Anruflisten zu unterrichten und darauf hinzuweisen, dass dritte Personen z. B. bei

Nutzung des Telefons Kenntnis über diese Informationen erlangen können, sowie geeignete Gegenmaßnahmen aufzuzeigen.

Direktansprechen / Direktantworten

Viele Endgeräte sind mit der Möglichkeit des Freisprechens ausgestattet, d. h., zum Führen eines Telefonates braucht der Hörer nicht abgenommen, sondern lediglich ein Knopf gedrückt zu werden. Wird für solche Endgeräte das Leistungsmerkmal *„Direkt- ansprechen/Direktantworten"* (Gegensprechanlage) eingerichtet, braucht auch die Leitungstaste nicht mehr betätigt zu werden: Ein ankommender Anruf schaltet das Endgerät automatisch ein – auch das eingebaute Mikrophon.

Typischerweise wird dieses Leistungsmerkmal für die Kommunikation zwischen „Chef" und Sekretariat eingerichtet, häufig wird es aber auch in Teamfunktion gewünscht: Der Chef kann damit kurze Rückfragen an seine Mitarbeiterinnen und Mitarbeiter richten, ohne dass diese den Hörer abzunehmen brauchen oder den Besprechungstisch verlassen müssen. Grundsätzlich ist es nicht möglich, mittels des direkten Ansprechens in bestehende Verbindungen einzutreten.

Um eine Beeinträchtigung der Persönlichkeitsrechte zu verhindern, wird empfohlen, bei Nebenstellenanlagen dieses Leistungsmerkmal nur dort frei zu schalten, wo es dringend benötigt wird und die Betroffenen informiert sind. Beim Direktansprechen sollte ein optisches und akustisches Signal erzeugt werden und möglichst das Leistungsmerkmal *„Ansprechschutz"* zur Verfügung stehen. Wird letzteres aktiviert, ist ein Direktansprechen dieses Anschlusses nicht möglich.

Konferenzschaltung

Ähnliche Beeinträchtigungen der Persönlichkeitsrechte können sich auch bei *Konferenzschaltungen* ergeben. Nicht alle Telekommunikationsanlagen machen durch ein obligatorisches, nicht zu unterdrückendes Signal deutlich, wenn ein neuer Teilnehmende in die Verbindung einbezogen wird oder wenn einer die *Telefonkonferenz* verlässt. Wird kein automatisches Signal erzeugt, wäre es z. B. möglich, dass die Teilnehmerin oder der Teilnehmer nur vorgibt, die Verbindung zu beenden, tatsächlich aber unbemerkt mithört.

Zeugenzuschaltung

Manche Telekommunikationsanlagen verfügen auch über das Leistungsmerkmal „*Zeugenzuschalten*“. Dabei wird ein anderer Teilnehmende oder ein Aufnahmegerät unbemerkt in eine bestehende Verbindung zur Dokumentation des Gesprächs eingeschaltet. Der Einsatz dieses Leistungsmerkmals ist nicht zulässig, und eine unbefugte Tonbandaufnahme nach § 201 Absatz 1 Nr. 1 StGB sogar strafbar (s. Kapitel 4.5). Eine Ausnahme für die Aufzeichnung von Anrufen gilt für Drohanrufe in sicherheitskritischen Bereichen. Sobald ein Gespräch als Drohanruf, z. B. eine Bombendrohung, erkannt wird, kann bei der Telefonzentrale ein Aufzeichnungsgerät zugeschaltet werden.

4.1.3 Voice over IP

Voice over IP (VoIP) oder *IP-Telefonie* oder aber auch *Internettelefonie* ist die aktuelle Evolutionsstufe auf der Entwicklungsleiter der Sprachkommunikation (zumindest im Bereich Festnetz) und beschreibt die Verwendung von Computernetzwerken als Transportmedium für Telefongespräche. Zielsetzung hierbei ist eine Reduktion der Kosten durch die Nutzung einer einheitlichen Infrastruktur, über die sämtliche Daten transportiert werden.

Der Übergang zu dieser Technologie ist nachvollziehbar, konsequent und logisch, leider aber auch mit ein paar Nachteilen gegenüber den ausschließlich für Telefongespräche vorgesehenen Netzen verbunden.

Sicherheit

Die Verschmelzung und damit die Vereinheitlichung des Kommunikationsmediums bergen zusätzliche Gefahrenpunkte. Wenn früher das Netz ausschließlich zum Telefonieren (und den zugehörigen Diensten) zur Verfügung stand, so war es nur mit großem technischem Aufwand und mit hohem Zusatzwissen möglich, Daten aus diesem Netz unbefugt abzufangen und zu verwerten, z. B. jemanden zu „belauschen“. Hybride Netze „erleichtern“ den Aufwand erheblich, Daten abzufangen, insbesondere, wenn die Netze keine Zugangsbeschränkung aufweisen.

Zudem sind die beiden populärsten Protokolle für VoIP, Session Initiation Protocol (SIP) und H.323, von Natur aus *geschwätzig* und per se nicht für die vertrauliche Kommunikation geeignet. Zu betonen ist, dass diese beiden Protokolle lediglich die Signalisierung der Verbindungen übernehmen, während der Transport des eigentlichen Gesprächs durch ein weiteres unverschlüsseltes Protokoll erfolgt. Die Konsequenz hieraus zeichnet sich recht deutlich ab: Entweder schafft man Vertraulichkeit im Datenverkehr, in dem man eine Verschlüsselung einführt, oder man sichert das gesamte Netz (dann ausschließlich für VoIP) gegen Eindringlinge ab – im Idealfall kommt beides kombiniert zum Einsatz.

Erfreulicherweise ist die verschlüsselte VoIP-Kommunikation bei TK-Anlagen heutzutage schon fast überall standardmäßig eingestellt und bietet somit schon von Beginn an einen gewissen Grundschutz. Weiterführende Informationen zur Verbesserung der Sicherheit, z. B. durch die Verwendung von Zertifikaten in den Endgeräten, hält das BSI in den Grundschutzkatalogen bereit (s. www.bsi.bund.de).

Vorteilhaft wirkt sich der Einsatz von VoIP auch bei der flexiblen und kurzfristigen Erweiterung einer bestehenden TK-Anlage aus. Binnen kürzester Zeit können größere Mengen von Nebenstellen – auch an weit entfernten Liegenschaften – mit wenig Aufwand integriert werden. Eine Anbindung über Weitverkehrsnetze darf aber in keinem Fall ohne zusätzlich Sicherheitsmechanismen wie z. B. Verschlüsselungstechniken erfolgen. Denkbar ist, die Netze zweier Liegenschaften über ein Virtual Private Network (VPN) zu koppeln.

Kommunikation und Infrastruktur

Telefon- und Datenverkehr gemeinsam über die vorhandene Netzwerkinfrastruktur zu befördern, da die Kapazität ausreichend vorhanden ist, scheint naheliegend und durchaus sinnvoll, wenn man die Effizienz steigern möchte. Allerdings kann man sich mit einer derartigen Entscheidung an anderer Stelle größere Probleme einhandeln. Denn die Trennung des Sprach- und Datenverkehrs ist ein wichtiger Bestandteil der Sicherheitsvorkehrungen für VoIP. Ein gemeinsames Sprach- und Datennetz ermöglicht einem Eindringling potenziell nicht nur den Diebstahl von Dokumenten, E-Mails oder ähnlichem Datenverkehr, sondern auch das Abhören von Telefongesprächen.

Die physikalische Trennung der Netze wäre als vorbeugende Maßnahme hier der beste Schritt, natürlich neben der bereits erwähnten obligatorischen Verschlüsselung. Somit könnte jedweder Übergriff aus einem der Netze durch die Separierung zunächst ausgeschlossen werden. Leider ist diese Maßnahme – häufig bedingt durch bauliche Begebenheiten – nicht immer so einfach und schon gar nicht kosteneffizient möglich. Sollten also die Gegebenheiten es nicht zulassen, ist die logische Trennung der Netze durch z. B. *Virtual Local Area Network* (VLAN) auch eine Maßnahme, die zumindest eine Trennung in abgeschwächter Form herbeiführt. In diesem Fall kann das Einbringen einer weiteren Hürde, wie z. B. Zertifikate auf den Endgeräten, hilfreich sein.

4.1.4 Telefax

Das Wort Telefax ist eine Verkürzung von Telefaksimile (wörtliche Übersetzung: Fernabbildung, daher auch die deutsche Bezeichnung Fernkopie). Die allgemein üblichere Bezeichnung Fax ist sowohl eine Verkürzung von Telefax als auch von Faksimile.

In Deutschland gewann das Faxgerät an Bedeutung, nachdem Gerichte den fristwahrenden Zugang eines Dokuments auch dann anerkannten, wenn der Schriftsatz innerhalb der Frist per Fax übermittelt worden war, obwohl es lediglich eine (Fern-) Kopie darstellt und das gesetzliche oder vertragliche Schriftformerfordernis im Sinne von § 126 Bürgerliches Gesetzbuch (BGB) nicht gewahrt wird; die Schriftform erfordert den Zugang einer Willenserklärung mit originaler Namensunterschrift. Eine Vielzahl von zivilrechtlichen Erklärungen, so zum Beispiel der Widerruf von Fernabsatzverträgen gemäß § 355 BGB, können rechtswirksam per Telefax abgegeben werden. Das Faxschreiben genügt der Textform im Sinne von § 126b BGB. Mit der allgemeinen Verbreitung des Internet ab Mitte der neunziger Jahre wurde der Telefaxdienst zunehmend durch E-Mail verdrängt. Die private Nutzung von Faxgeräten verschiebt sich zugunsten von Online-Faxdiensten, die zum Teil sogar kostenfrei zu nutzen sind.

Die Beweistauglichkeit von Faxen ist beschränkt. Da hier nur ein Abbild der händischen Unterschrift übertragen wird (sehr geringe Auflösung, keinerlei Information über Druck sowie Schriftführung und Geschwindigkeit), sind diese Unterschriften für eine Schriftvergleichung kaum geeignet, so dass ein Echtheitsnachweis nur schlecht zu

führen ist. Ein weiteres Problem besteht darin, dass die Gegenstation nicht sicher identifizierbar ist.

Das wird von dubiosen Firmen genutzt, die unverlangt Werbung oder sogar unseriöse bis betrügerische Vertragsangebote zuschicken (mit unterdrückter Faxnummer).

Datenschutzrechtlich ist der Faxdienst schon deshalb problematisch, weil die sichere Nutzung nicht gewährleistet ist. Ein Fax kommt in der Regel beim Empfänger offen an – also wie eine Postkarte – und ist damit für jeden lesbar, der sich in der Nähe des empfangenden Faxgerätes befindet.

Fax-Werbung ist unzulässig, wenn man nicht vorher eingewilligt hat. Erhält man dennoch Werbung per Fax, kann man in der Regel gegen die Verantwortlichen zivilrechtlich vorgehen und Unterlassung der Werbung verlangen oder eine Stelle einschalten, die die werbende Stelle abmahnt. Unterstützung dafür erhält man bei den Verbraucherschutzverbänden, bei der Zentrale zur Bekämpfung unlauteren Wettbewerbs e.V. sowie bei der BNetzA.

In vielen Fällen ist es jedoch sehr schwierig, Rechtsansprüche durchzusetzen. Die Absender der rechtswidrigen Werbefaxe, die oft nicht identisch mit den Werbenden sind, lassen sich – wenn überhaupt – häufig nur mit großem Aufwand ermitteln. Vielfach werden Faxnummern nicht gezielt angewählt, sondern durch Computer zufällig gewählt. Wegen der einfachen und allseits bekannten Nummernstruktur bedarf es nur eines kleinen Programms, das automatisch Nummern erzeugt. An die künstlich erzeugten Verbindungsnummern werden dann Faxe versandt – in der Hoffnung, dass sich hinter möglichst vielen Nummern tatsächliche Anschlüsse verbergen. Die BNetzA hält unter www.bundesnetzagentur.de ein Formular bereit, mit dem jeder Anzeige erstatten kann, der unerlaubte Faxwerbung erhält. Mit diesem Formular werden die Angaben erfragt, die die BNetzA für ein Bußgeldverfahren wegen unerlaubter Faxwerbung benötigt.

Daneben kann man sich – wie bei anderer Werbung auch – in Listen gegen Werbung eintragen lassen (z. B. Robinsonliste, s. Kapitel 3.4). Da Fax-Werbung im Gegensatz zur Briefwerbung jedoch von vornherein nur mit Einwilligung erlaubt ist, sind solche Lis-

ten nicht immer hilfreich. Manchmal werden sogar Gebühren für die Eintragung verlangt, was unseriös ist. Es ist auch nicht ausgeschlossen, dass Listen gegen Werbung missbräuchlich genutzt werden, um gerade den eingetragenen Personen Werbung zu senden.

4.1.5 Virtuelle Telefonanlagen

Neudeutsch *IP-Centrex* bezeichnet die Übernahme des althergebrachten Centrex-Prinzips (Central Office Exchange) in das Zeitalter des Internetprotokolls. Bereits in den 50er und 60er Jahren des letzten Jahrhunderts hatte man in den Vereinigten Staaten begonnen, technische Einrichtungen in Unternehmen auszulagern, um Kosten zu sparen und wirtschaftlicher zu agieren. Unter dem Begriff Centrex begann man, den Aufbau und die Wartung der klassischen Telefonanlage dem TK-Anbieter zu überlassen, der den Betrieb in seinen eigenen Räumlichkeiten erledigen konnte.

Was damals technisch (wegen Verkabelung) noch schwierig umzusetzen war, ist heute leichter, da keine direkte Leitungsverbindung mehr notwendig ist. Durch die Deregulierung des Telekommunikationsmarktes und die Vereinfachung des Anschlusses wurde eine Renaissance dieser Technik ausgelöst, so dass diese *virtuellen Telefonanlagen* heute als äußerst flexibel und kostengünstig gelten.

Anbindung des Anschlussinhabers

Die virtuellen Telefonanlagen basieren heute fast ausnahmslos auf der VoIP-Technologie, meistens unter Verwendung des Session Initiation Protocols (SIP). Der TK-Anbieter hält in seinem Rechenzentrum für die jeweiligen Kundinnen und Kunden eine eigene virtuelle Telefonanlage bereit, die die Kunden (oder Anschlussinhaber) über diverse Wartungsschnittstellen (z. B. Weboberfläche) selbst konfigurieren und betreuen können. Der technische Betrieb sowie die Wartung der Technik der Anlage obliegen dem Anbieter. Die Kundin bzw. der Kunde muss in den Räumlichkeiten lediglich die notwendige Anzahl an Endgeräten sowie einen geeigneten Internetanschluss bereithalten. Maßgeblich beim Internetzugang ist der Datendurchsatz; ist dieser zu gering, kann es zu einer eingeschränkten Erreichbarkeit kommen. Das Einbringen neuer Endgeräte kann bzw. muss die betreffende Person selbst durchführen.

In technischer Hinsicht ist bei der Verwendung einer virtuellen Telefonanlage als grundsätzlich kritisch zu bewerten, dass die Anbindung der Telefone an die Anlage oft unverschlüsselt erfolgt. Das verwendete Protokoll SIP ist gegen unerwünschte Zuhörer nicht gerüstet und mit einfachsten Mitteln zu manipulieren. Der Einsatz einer solchen Anlage muss demnach reiflich überlegt sein, auch im Hinblick auf einen möglichen Standort der Server, auf denen die Anlage betrieben wird. Der Standort des Rechenzentrums, das den Betrieb der Anlage sichert, sollte vertraglich festgehalten werden, da es unter Umständen rechtliche Implikationen geben kann, wenn es um Daten geht, die innerhalb der TK-Anlage gespeichert werden. Hiervon sind nicht nur die Anruflisten und Einzelverbindungsnachweise betroffen, sondern möglicherweise im System gespeicherte Adress- und Telefonbücher sowie Faxe.

4.1.6 Speicherung von Verkehrsdaten

Beim Betrieb von TK-Anlagen werden in der Regel systemintern Daten protokolliert. Diese Protokolle enthalten (je nach Konfiguration) Angaben zu Telefongesprächen, wie z. B. beteiligte Nebenstelle, angerufene Telefonnummer, Uhrzeit und Länge des Gesprächs, Tarifangaben usw. Notwendig sind diese Daten, um z. B. Gespräche abrechnen oder auch um einen ordnungsgemäßen Betrieb der Anlage sicherstellen zu können. Diese Protokollierung ist aus datenschutzrechtlicher Sicht als Erhebung und Speicherung von sog. Verkehrsdaten (s. Kapitel 2.6) zu werten. Dabei sind entweder die Vorgaben des TKG oder des BDSG zu beachten. Nachfolgend werden zwei prinzipielle „Betriebsarten“ (sowie die Kombination aus beiden Möglichkeiten) von TK-Anlagen erläutert. Welche Rechtsgrundlagen jeweils zur Anwendung kommen, hängt davon ab, ob es „Dritten“ gestattet oder möglich ist, eine TK-Dienstleistung in Anspruch zu nehmen.

Betrieb einer TK-Anlage für eigene Zwecke

Der Betrieb einer TK-Anlage für eigene Zwecke liegt vor, wenn diese ausschließlich der Sicherstellung der unternehmensinternen Kommunikation (einschließlich der dienstlichen Telefongespräche ins öffentliche Fernmeldenetz) dient und keine privaten Gespräche zulässig sind. In diesem Fall unterliegen die Erhebung, Speicherung und Nutzung der Verkehrsdaten dem BDSG. Das Verbot zur privaten Nutzung kann z. B. durch geeignete Dienstanweisungen geregelt sein.

Für die Protokollierung der Verkehrsdaten gebietet § 3a BDSG Datensparsamkeit. Es dürfen nur solche Daten erhoben werden, die für den Betrieb notwendig sind, wie z. B. abrechnungsrelevante Daten. Hingegen dürfen interne Gespräche, die keine Kosten verursachen, nicht protokolliert werden. Bei Nutzung der Verkehrsdaten zu statistischen Auswertungen (Beispiel: Erstellung einer Statistik zur Verteilung der Gesprächskosten, aufgeteilt nach Abteilungen) sind diese so früh wie möglich zu anonymisieren. Weiterhin ist die Zweckbindung der erhobenen Verkehrsdaten strikt zu beachten. Werden Daten zu Abrechnungszwecken erhoben, dürfen sie nicht für weitere Zwecke genutzt werden; so ist es z. B. nicht statthaft, die Verkehrsdaten zur Leistungsüberwachung des Anschlussinhabers heranzuziehen. Über die Erhebung, Speicherung und Nutzung der Verkehrsdaten sind die Betroffenen in geeigneter Weise zu unterrichten.

Personen, die für den Betrieb der TK-Anlage zuständig und verantwortlich sind, müssen bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichten werden (§ 5 BDSG). Personen, die für den Betrieb der TK-Anlage zuständig und verantwortlich sind, ist es untersagt, personenbezogene Daten, die beim Betrieb der TK-Anlage erhoben und gespeichert werden, unbefugt zu nutzen.

Dem Betreiber der TK-Anlage obliegt gemäß § 9 BDSG die Pflicht, technische und organisatorische Maßnahmen vorzusehen, die notwendig sind, um die TK-Anlage entsprechend den Anforderungen des BDSG zu betreiben. So ist z. B. der Zugriff auf die TK-Anlage zu schützen (Betrieb in einem verschlossenen Raum, Zutrittskonzept, Zugriffsrechte auf die Anlage z. B. durch Passwortschutz), um unerlaubte Zugriffe und Manipulationen möglichst auszuschließen.

Betrieb einer TK-Anlage für „außen stehende Personen“ (Dritte)

Eine TK-Anlage kann auch mit dem Ziel betrieben werden, Dritten (also außen stehenden Personen) eine TK-Dienstleistung anzubieten. Dies ist zum Beispiel in einem Krankenhaus oder in einem Hotel der Fall, wenn Gästen eine TK-Dienstleistung angeboten werden soll. Nach § 3 Nr. 6 TKG ist *Diensteanbieter* jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Nach § 3 Nr. 10 TKG ist das „geschäftsmäßige Erbringen von Telekommunikationsdienstleistungen“ das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Demnach ist es unerheblich, ob für

die Nutzung der TK-Anlage ein Entgelt (Gesprächsgebühren) vom Nutzenden erhoben wird. Der Betreiber der TK-Anlage ist demnach Telekommunikationsdiensteanbieter mit der Folge, dass statt des BDSG die Regelungen des TKG anzuwenden sind.

Die in der TK-Anlage erhobenen Verkehrsdaten wie Nummer bzw. Kennung der beteiligen Anschlüsse sowie Datum und Uhrzeit der Verbindung dürfen nur zur Gesprächsabrechnung nach § 97 TKG verwendet werden. Dazu hat der TK-Anlagen-Betreiber nach Beendigung der Verbindung unverzüglich die für die Abrechnung notwendigen Daten zu ermitteln und die nicht erforderlichen Daten umgehend zu löschen. Diese Abrechnungsdaten sollten höchstens bis zu 3 Monate nach Rechnungsstellung gespeichert bleiben (s. Kapitel 2.7). Wenn Daten für eine Störungsbeseitigung benötigt werden, dürfen diese ohne konkreten Anlass nur für kurze Zeit – bis zu sieben Tage – gespeichert werden (s. Kapitel 2.10).

Betrieb einer TK-Anlage sowohl für eigene Zwecke als auch zur Nutzung durch Dritte
In der Praxis sind beide *Betriebsarten* häufig nicht getrennt: Vielmehr dient der Betrieb der TK-Anlage sowohl der unternehmensinternen Kommunikation als auch der Erbringung von TK-Diensten für Dritte, wenn z. B. in einem Unternehmen auch Privatgespräche erlaubt sind. Da die Verkehrsdaten nach unterschiedlichen Rechtsgrundlagen gespeichert werden, sind die Datensätze bereits bei der Erhebung zu kennzeichnen. Diese „Markierung des Verkehrsdatensatzes“ lässt sich z. B. mittels Vorwahl einer Ziffer realisieren. Wird etwa bei Privatgesprächen stets eine „9“ vorgewählt, so kann bei der Datenerhebung und -verarbeitung bereits zwischen Privat- und Dienstgesprächen unterschieden werden.

Planung und Beschaffung von TK-Anlagen
Bereits im Vorfeld der Beschaffung einer neuen Anlage müssen die technischen Vorgaben, die sich aus dem BDSG und TKG ergeben, zwingend berücksichtigt werden, um später einen datenschutzgerechten Betrieb gewährleisten zu können. Die Anlage ist so zu konfigurieren, dass ausschließlich Daten im zulässigen Rahmen erhoben und gespeichert werden. Weiterhin muss das datenschutzkonforme Löschen der Protokolldateien möglich sein; entsprechende automatisierte Löschroutinen unterstützen den datenschutzgerechten Betrieb der Anlage.

4.1.7 Besonderheiten für Bundesbehörden

Der Betrieb von TK-Anlagen bei Bundesbehörden ist durch die Verwaltungsvorschrift „Richtlinie über die Einrichtung und Benutzung dienstlicher Telekommunikationseinrichtungen und die dienstliche Benutzung privater Telekommunikationseinrichtungen in der Bundesverwaltung (Richtlinie Telekommunikation Bund – RLTk-Bund) verbindlich geregelt. Primäre Aufgabe dieser Richtlinie ist es, den wirtschaftlichen Betrieb von TK-Anlagen im behördlichen Umfeld zu regeln. Nach diesen Vorgaben ist ausschließlich die dienstliche Nutzung von TK-Anlagen zulässig. Eine private Nutzung kann jedoch zugelassen werden, wobei die entstehenden Kosten der geführten Privatgespräche durch die Nutzenden zu tragen sind. Die RLTk-Bund gilt grundsätzlich für alle Telekommunikationsdienste, die von Bundesbehörden genutzt werden. Darunter fällt insbesondere auch der Betrieb von dienstlichen TK-Anlagen, die Zugang zu einem öffentlichen Telekommunikationsnetz haben. Die RLTk-Bund enthält als Anlagen insgesamt vier Ausführungshinweise. Der aus Datenschutzsicht Wichtigste – enthalten in Anlage 1 – regelt verbindlich für alle Bundesbehörden den zulässigen Umfang der Datenerhebung, -speicherung und -nutzung.

Datenschutz

Verkehrsdaten dürfen beim Betrieb von TK-Anlagen ausschließlich im Rahmen der betrieblichen Notwendigkeit und der wirtschaftlichen Verwertbarkeit gespeichert werden. Sie sind demnach auch nur in dem Maß zu erheben, wie dies zur Kontrolle der Einhaltung der RLTk-Bund und zur Abrechnung von privaten Gesprächen erforderlich ist.

Eingehende Anrufe in der TK-Anlage oder kostenneutrale anlageninterne Gespräche dürfen nicht protokolliert werden. Ebenso wenig dürfen Daten von externen dienstlichen Gesprächen erhoben und gespeichert werden, wenn die Gesprächsgebühren in ein öffentliches Telefonnetz pauschal abgegolten werden (sog. *Flatrate-Tarife).* Bei der Datenerhebung und -speicherung ist zwischen der Erfassung der dienstlichen Verbindungen und der bei privater Nutzung, wenn diese gestattet ist, zu differenzieren. Für beide Nutzungsfälle sollte die Speicherung von Kommunikationsdaten generell auf maximal drei Monate beschränkt sein.

Zur Gewährleistung des sicheren Betriebs der TK-Anlage (einschließlich der Wartung) sowie zur statistischen Analyse ist die Erhebung und Auswertung von personenbezogenen Daten zulässig, wenn diese zum frühestmöglichen Zeitpunkt anonymisiert werden und somit kein Rückschluss mehr auf Einzelpersonen gezogen werden kann. Als Beispiel sei hier die Analyse von Telefonkosten nach Abteilungen oder Referaten einer Behörde genannt.

Dienstliche Telefonate

Generell dürfen ausschließlich abrechnungsrelevante Daten erfasst und gespeichert werden. Bei externen dienstlichen Verbindungen ist es zulässig, das Datum (jedoch nicht die Uhrzeit), die Teilnehmernummer, die vollständige Zielrufnummer sowie die Tarifeinheiten/ Leistungsentgelte zu erfassen und zu speichern. Diese Daten dürfen nicht mit anderen Dateien verknüpft oder zu anderen Zwecken als der Entgeltabrechnung verwendet werden (Beispiel: Verwendung zur Leistungskontrolle einer beschäftigten Person).

Eine weitere Besonderheit stellen in diesem Zusammenhang die Dienstanschlüsse der Personen dar, die aufgabenbezogen nicht der allgemeinen Dienstaufsicht unterliegen, wie z. B. Vertreter des Personalrates oder der behördliche Datenschutzbeauftragte. Hier ist lediglich die Erhebung und Speicherung der Tarifeinheiten bzw. der Verbindungsentgelte zulässig, so dass die Verkehrsdaten keine weiteren Rückschlüsse zulassen. Der Dienstherr hat regelmäßig mittels Stichproben zu überprüfen, ob die TK-Anlage von den Mitarbeiterinnen und Mitarbeitern ausschließlich zu dienstlichen Zwecken genutzt wird. Das Verfahren hierzu sollte mit dem Personalrat abgestimmt und in entsprechenden Dienstvereinbarungen umgesetzt werden. Die Betroffenen sind in geeigneter Weise über das Verfahren und die Ausführung zu informieren.

Private Nutzung der TK-Anlage

Der Dienstherr kann die private Nutzung einer dienstlichen TK-Anlage erlauben. In diesem Fall sind die abrechnungsrelevanten Verkehrsdaten zu erheben, um die Kosten der Privatgespräche mit Nutzenden abrechnen zu können. Dazu sind diese Privatgespräche gesondert zu kennzeichnen, was z. B. durch Vorwahl einer Ziffer geschehen kann. Bei diesen Verkehrsdaten sind die letzten drei Ziffern der angerufenen Anschlüsse zu unterdrücken, d. h., die TK-Anlage ist so zu konfigurieren, dass die Zielrufnummer bei Privat-

gesprächen bereits in gekürzter Form erhoben wird. Der Auszug zur Abrechnung von Privatgesprächen darf nur von besonders beauftragten Personen gefertigt werden, und eine mögliche Kenntnisnahme durch Dritte muss bereits durch technische und organisatorische Maßnahmen ausgeschlossen sein. Nach der Abrechnung sind die Verkehrsdaten unverzüglich zu löschen sowie eventuell vorhandene Papierausdrucke zu vernichten. In der Vergangenheit wurden aus datenschutzrechtlicher Sicht für private Gespräche die Nutzung sog. Calling-Cards empfohlen, bei denen ein vorausbezahltes Gesprächsguthaben bei einem Anbieter erworben wird, das bei Nutzung der dienstlichen TK-Anlage abtelefoniert wird. Die Abrechnung des Gesprächsguthabens erfolgt dann direkt beim Anbieter der Karte und nicht über die Bundesbehörde, so dass die Privatgespräche durch die Dienststelle weder zu protokollieren noch abzurechnen sind. Aufgrund der Verbreitung von Mobilfunktelefonen haben Callingcards in der Praxis kaum noch eine praktische Bedeutung.

4.2 Mobile Kommunikation

Längst ist es selbstverständlich, dass Telefone nicht mehr schnurgebunden sind und über einen erheblichen Funktionsumfang verfügen. Neben der reinen Sprachübertragung sind heute mobile Datenanwendungen wie z. B. Internetzugriff üblich. Als Geräte für die mobile Kommunikation werden neben Handys und Smartphones auch Tablets und Notebooks mit Mobilfunkschnittstellen („Surfstick“) verwendet, die sowohl mobile Telefonie als auch Datenanwendungen unterstützen. Aus technischer Sicht differenziert man bei der Mobilkommunikation zwischen verschiedenen Standards wie z. B. DECT, WLAN, GSM, UMTS und LTE . Die Verfahren unterscheiden sich dabei z. B. durch die Größe der versorgten Fläche eines Systems (Beispiel: DECT und WLAN sind nur zur Versorgung relativ kleiner Bereiche geeignet) und in den möglichen Datenübertragungsraten.

Im Gegensatz zur drahtgebundenen Telekommunikation wird die Sprach- und Datenübertragung bei der Mobilkommunikation per Funkanbindung realisiert; dieser zusätzliche Übertragungsweg muss also gegen mögliches Abhören und Manipulation geschützt werden. Daneben ist es bei großflächigen Mobilfunksystemen wie z. B. GSM, UMTS undLTE prinzipiell möglich, geografische Bewegungsprofile der Nutzerinnen

und Nutzer zu erstellen oder den aktuellen Standort zu ermitteln. Diese Beispiele zeigen, dass neben dem erheblichen Komfort, den diese Systeme bieten, der Datenschutz bei der Nutzung von Mobilfunksystemen nicht außer Acht gelassen werden darf.

4.2.1 Drahtlose Kommunikation für die Telefonie im Festnetz

Die drahtlose Kommunikation ist, bestimmt durch die Natur der Signalübertragung, schon seit jeher eine fehleranfällige und sicherheitskritische Technologie. Im Laufe der Zeit hat jedoch auch hier die Innovation Einzug gehalten, zumindest was die zugrunde liegenden Standards betrifft.

Die Zeiten, in denen es nur eines einfachen Scanners, d. h. eines in jedem Fachgeschäft erhältlichen Spezialempfängers, bedurfte, um schnurlose Telefone abzuhören, sind mit digitalen Funktelefonen des *Digital-Enhanced-Cordless-Telecommunications-Standards* (DECT) weitgehend vorbei. Der technische Aufwand für das Abhören von Gesprächen auf der Luftschnittstelle ist hierbei etwas höher, aber dennoch mit vertretbarem Aufwand grundsätzlich möglich. Dies beruht zunächst einmal darauf, dass die auf dem Funkweg übertragenen Nachrichten nicht mehr analog, sondern digital codiert, d. h. zusätzlich digital aufbereitet, sind. Ein einfaches Abhören mit preiswerten Geräten ist also nicht mehr möglich, da nicht nur das Signal abgefangen werden muss, sondern auch noch zusätzlich die Nachricht in ein hörbares Format „zurückübersetzt“ werden muss. Wer ein besonders hohes Sicherheitsbedürfnis hat, sollte sich über die Verschlüsselungsverfahren informieren, die er für seine Telefonate nutzen kann.

Bereits im Jahre 2009 hat sich gezeigt, dass über DECT geführte Telefonate mit einem Kostenaufwand von wenigen hundert Euro abgehört werden können. Dies liegt darin begründet, dass die meisten Hersteller aktueller DECT-Produkte wider besseres Wissen die optional für DECT standardisierte Verschlüsselung nicht in den Geräten vorsehen und/oder einsetzen. Auch mit heutigen Software Defined Radio-Empfängern ist der Empfang von unverschlüsselten Telefonaten über DECT am Computer mit überschaubarem Aufwand möglich.

Die Standardisierungsgremien setzen unterdessen auf den Nachfolger des DECT-Standards, die bereits Ende 2006 vorgestellte *Cordless Advanced Technology – internet and quality* (CAT-iq). Diese Technologie unterscheidet sich nicht maßgeblich vom Vorgänger, bietet allerdings einige Vorteile in Sachen Komfort bzw. Anwendungsmöglichkeiten und Sicherheit. Es kommt zwar immer noch der altbewährte Algorithmus zum Einsatz, womit das System zu knacken ist, aber ein Fortschritt ist der zwingende Einsatz der Verschlüsselung in den Endgeräten. Darüber hinaus ermöglicht die Technologie dank integrierter Internetfähigkeit eine deutlich vereinfachte Aktualisierung der Geräte.

4.2.2 Mobiltelefon und Smartphone

Kaum eine Technik in der Kommunikation hat sich in den letzten Dekaden so rasant entwickelt wie der Mobilfunk. Galt zunächst der analoge Mobilfunk sowie das *Global System for Mobile Communications* (GSM) noch als weitgehend sicher gegenüber unerwünschten Zuhörern, so hat sich dies in den letzten Jahren stark verändert.

GSM

In den Mobilfunknetzen nach dem GSM-Standard werden Sprache und Daten digital übertragen. Zusätzlich wird mit einem kryptographischen Algorithmus verschlüsselt, wobei der Schlüssel häufig gewechselt wird. Dies gilt nicht nur für die Gesprächsinhalte, auch die Teilnehmerkennung wird in der Regel nicht im Klartext übertragen. Das heißt, wer Datenpakete eines Gesprächs auf der Luftschnittstelle abfängt, kann nur schwer erkennen, wer der Urheber der Daten ist. Der verwendete kryptographische Algorithmus ist allerdings etwas in die Jahre gekommen und kann mit der Weiterentwicklung der PC- und Signalprozessortechnik nicht mehr ganz Schritt halten. Dies wurde eindrucksvoll im Dezember 2009 demonstriert, als man den Algorithmus öffentlichkeitswirksam knackte. Ein verbesserter Algorithmus wurde inzwischen eingeführt, so dass man inzwischen meist mit verbesserter Verschlüsselung telefoniert – vorausgesetzt das Netz und das Handy unterstützen den neuen Standard. Zudem gibt es Fälle, z. B. in manchen ausländischen Netzen, in denen die Verschlüsselung nicht aktiv ist. Dann ist ein Mithören – um einiges einfacher – möglich.

UMTS

Der Nachfolger *Universal Mobile Telecommunications System* (UMTS) bringt hier nur bedingt Abhilfe. Bisher gelang es noch nicht, die Verschlüsselung bzw. die Sicherheitsaushandlungen von UMTS direkt zu unterwandern, womit das gesamte System derzeit als relativ sicher angesehen werden kann. Jedoch bieten die UMTS-Endgeräte eine Komfortfunktion, die sie wiederum anfällig macht. Sollte die Versorgung mit UMTS mal nicht sichergestellt sein, kann fast jedes UMTS-Gerät auf das GSM-System zurückgreifen und ist somit denselben Gefahren ausgesetzt wie die Vorgängergeräte. Der zusätzliche Aufwand, den ein Eindringling hier mit dem Blockieren des UMTS-Signals bewältigen muss, ist überschaubar, so dass auch der Sprach- und Datenverkehr von UMTS-Endgeräten abgehört werden kann.

LTE

Die aktuelle Mobilfunkgeneration Long Term Evolution (LTE) ermöglicht besonders schnelles Surfen mit dem Smartphone. Hier gibt es einige Fortschritte bei den Sicherheitsaspekten, allerdings wurden auch einige Probleme von den Vorgängergenerationen „geerbt". So besteht auch hier die Möglichkeit, durch Störung der LTE und UMTS-Funksignale auf eine GSM-Kommunikation zurückzufallen.

Endgeräte

Allerdings ist dies nur die halbe Wahrheit. Zu den Gefahren des Kommunikationsmediums (hier: GSM, UMTS, LTE oder die fünfte Generation Mobilfunk 5G) kommt noch das Gefahrenpotenzial des Endgerätes hinzu.

Endgeräte sind heutzutage nicht mehr nur profane Telefone, die heute überwiegend genutzten Smartphones besitzen Funktionalitäten ähnlich eines Computers, eine Verbindung mit dem Internet ist meist permanent aktiv. In der Regel sind Smartphones durch kleine Programme (sog. Apps) erweiterbar.

Die Angriffsfläche der Endgeräte ist durchaus vielschichtig und nicht nur auf den Mobilfunk begrenzt, da einige der Geräte auch in anderen Kommunikationsnetzen heimisch sind. Grundsätzlich kann man drei Ebenen identifizieren:

- Die *Hardwareplattform,* also die technischen Bestandteile, die die Kommunikation mit unterschiedlichen Netzen und Technologien (GSM, UMTS, WLAN, Bluetooth etc.) erlaubt, sowie die zugehörigen Rechen- und Speichereinheiten,
- das *Betriebssystem,* das den Betrieb des Gerätes sowie eine mögliche Erweiterung durch Applikationen Dritter erlaubt und
- *Applikationen* (Apps), mit denen der Nutzer die Aufgaben des täglichen Lebens ausführen und erledigen kann.

Da man datenschutzrechtlich an die Hardware zunächst nur die Forderung stellen kann, möglichst auf dem neuesten Stand zu sein und gegen unbefugten Zugriff zu schützen, sind noch die beiden Ebenen *Betriebssystem* und *Applikationen* näher zu beleuchten (s. Kapitel 4.2.6).

4.2.3 Leistungsmerkmale

Grundsätzlich gelten für die meisten Mobilfunknetze und deren Endgeräte genau die gleichen Leistungsmerkmale wie für die Telekommunikationsanlagen (s. Kapitel 4.1.2). Darüber hinaus verfügen einige Netze über zusätzliche *ergänzende Dienstmerkmale,* die es (zum Teil) ausschließlich innerhalb der Mobilfunknetze gibt.

Automatische Rufannahme

Um das Leben komfortabler zu gestalten, bieten viele Mobiltelefone ein Leistungsmerkmal, das die automatische Annahme von Anrufen ermöglicht. Gedacht ist diese Funktion für den Einsatz z. B. im Auto, also immer dann, wenn man gerade keine Hand frei hat, um einen ankommenden Anruf am Telefon per Tastendruck anzunehmen. Da bei diesem Leistungsmerkmal häufig keine dauerhafte optische Signalisierung im Display über den eingeschalteten Modus erfolgt, kann eine unbemerkt aufgebaute Verbindung zum Mithören aller Gespräche in der unmittelbaren Umgebung, in dem sich das Mobiltelefon befindet, benutzt werden. Das Mobiltelefon wird praktisch zur Wanze für jedermann, da das Telefon bei Anruf nicht einmal klingelt.

Bei einem Mobiltelefon lässt sich eine bestehende Verbindung am Display erkennen. Es besteht jedoch auch die Möglichkeit, jemanden ein umgebautes Gerät unterzu-

schieben, bei dem das Display keine Aktivität anzeigt, obwohl die Raumgespräche abgehört werden. Es ist daher ratsam, bei wichtigen persönlichen Gesprächen das Smartphone auszuschalten.

Schnittstellen

Ein Mobiltelefon, das in der Vergangenheit nur zum Telefonieren diente, wird heute dank neuer Fähigkeiten zur Kommunikationszentrale. Dabei speichert es Adressen, Termine, nimmt über die Infrarotschnittstelle, Bluetooth oder WLAN Kontakt zu anderen Geräten auf und ermöglicht dank Datendienst wie GPRS und HSPA auch unterwegs die Verbindung zum Internet. Gefahren wie Viren, Würmer oder Trojaner, die bisher nur bei PCs zu beachten waren, sind schon lange keine Fiktion mehr, wenn aktive Inhalte ausgeführt werden oder reihenweise Applikationen eigenverantwortlich installiert werden können. Dies erfordert insgesamt einen aufmerksamen und fast schon fachkundigen Nutzer, der Schnittstellen und Dienste des Mobilgeräts versteht und im Griff hat, um hier einen unberechtigten oder ungewollten Datenabfluss zu verhindern.

Videotelefonie

Ebenso wie die Sprachtelefonie Gefahren birgt, ist auch die Gesprächsführung per Videoverbindung hiervon betroffen. Gerade die automatische Rufannahme ist in diesem Fall als besonders kritisch zu beurteilen, da der Zuhörer nicht nur den Ton, sondern auch ein Bild erhält, ohne dass der Betroffene davon etwas mitbekommt.

4.2.4 Ortung bei Telemediendiensten

In Kapitel 2.8 wurde die Rechtslage erläutert, unter welchen Voraussetzungen die Standortdaten von einem Telekommunikationsnetz oder Telekommunikationsdienst erhoben bzw. verwendet werden. Eine Ortung ist bei modernen Endgeräten wie z. B. Smartphones möglich, da in vielen Geräten eine Satellitenortung, insbesondere Global Positioning System (GPS) und WLAN-Ortung voreingestellt sind. Dies ermöglicht oft eine recht genaue Standortbestimmung. Werden diese Daten für Telemedien verwendet wie z. B. bei Apps, findet das TKG keine Anwendung.

Im TMG und BDSG gibt es – im Unterschied zum TKG – keine besonderen Regelungen für die Nutzung von Standortdaten. Bieten Anbieter ihren Dienst nicht von Deutschland aus an, ist in der Regel deutsches Datenschutzrecht überhaupt nicht durchsetzbar.

Für Smartphones gibt es unzählige Apps, die auch Standortdaten nutzen; für die Übertragung dieser Standortdaten fallen durch die meist vorhandene Internetflatrate keine Kosten an. Die Standortdaten können genutzt werden, um das lokale Wetter oder die nächsten Filiale eines Unternehmens anzuzeigen, aber auch, um lokal angepasste Werbung zur Finanzierung der App zu präsentieren. Weiterhin gibt es Anwendungen, bei denen alle Mitglieder einer Gruppe den Standort der anderen Mitglieder auf einer Karte angezeigt bekommen. Selbst die Smartphone-Betriebssysteme sind, was Standortdaten betrifft, recht neugierig; auch hier sollten die Einstellungen betrachtet werden.

Bei den Telemedien, insbesondere, wenn sie nicht aus Europa angeboten werden, sollte man sich bewusst machen, dass Protokolle mit personenbezogenen oder personenbeziehbaren Daten oft lange gespeichert werden. Somit können Bewegungsprofile entstehen, die wiederum mit anderen Daten verknüpfbar sind. Daher ist es wichtig, die Datenschutzerklärung durchzulesen, bevor man in die Nutzung einer App einwilligt. Gesundes Misstrauen ist ratsam, da manche Nutzungsbedingungen nur vortäuschen, die Daten zu anonymisieren, während sie in Wirklichkeit unter einem anderen Identifikationsmerkmal, einem sog. Pseudonym, gespeichert werden.

Informationen über den Standort geben auch ein Stück des Lebenswandels preis. Gerade bei Diensten wie z. B. den Sozialen Netzwerken, bei denen man seinen Standort anderen mitteilt, sollte man sich stets überlegen, ob dies wirklich gewollt ist und ob man weiß, wer diese „Anderen“ sind. Generell empfiehlt es sich, die Ortungs- bzw. GPS-Funktion zu deaktivieren und sie nur bei Bedarf einzuschalten.

4.2.5 Kurznachrichten

Bei einem Telefonat können Anrufende bestimmen, ob die Rufnummer übertragen wird oder nicht (s. Kapitel 2.12). Bei Kurzmitteilungen (SMS) wird die Rufnummer immer übertragen. Dies mag Smartphone-Besitzern, die diesen Dienst nur gelegentlich nut-

zen, nicht bewusst sein und kann somit zu einer ungewollten Weitergabe der Mobilfunknummer führen.

Eine SMS kann auch mit dem PC über das Internet oder über ein Modem versandt werden. Auf diesem Wege können auch anonyme Mitteilungen übermittelt werden. Eine SMS ist – wie auch eine Postkarte – nicht immer zurückverfolgbar. Auch die Unterschrift, also die Rufnummer des Absenders, ist bei einigen Diensten frei wählbar. Eine in der SMS angegebene Absenderrufnummer ist also nicht absolut verlässlich, sie könnte auch manipuliert sein.

Die SMS wird zwar noch gelegentlich verwendet, hat aber verschiedene Nachfolger gefunden. Die MMS (Multimedia Messaging Service) ist in einigen Punkten mit der SMS vergleichbar, bietet zusätzlich aber die Möglichkeit, Bilder und andere Inhalte zu versenden. Die mobilen Messenger-Dienste, die man meist kostenlos über ein Smartphone mit Datenflatrate nutzen kann, sind jedoch inzwischen deutlich populärer geworden und laufen der SMS den Rang ab. Diese werden in Abschnitt 4.6 besprochen.

4.2.6 Betriebssysteme und Applikationen

Im Folgenden werden die Bereiche Betriebssysteme und Applikationen erläutert.

Betriebssystem

Nach der Definition der DIN-Sammlung 44300 wird das Betriebssystem definiert als „*die Programme eines digitalen Rechensystems, die zusammen mit den Eigenschaften dieser Rechenanlage die Basis der möglichen Betriebsarten des digitalen Rechensystems bilden und die insbesondere die Abwicklung von Programmen steuern und überwachen.*“ Diese doch sehr abstrakte Formulierung beschreibt das Betriebssystem als unsichtbaren „Vermittler“ zwischen Hardware und Software.

Im speziellen Fall des Mobiltelefons bekommt das Betriebssystem noch eine zusätzliche Aufgabe. Es agiert als „Mittelsmann“ zwischen dem *digitalen Rechensystem* (also dem Smart-) und der *Mobilfunkeinheit* (dem -phone) und stellt damit Nutzenden die Möglichkeiten eines Telefons zusätzlich zur Verfügung. Nur gemeinsam mit einer Mobilfunk-

verbindung kann das Hosentaschenrechensystem als Smartphone funktionieren. Die Nutzenden selbst haben auf die Mobilfunkeinheit nur mittelbar Einfluss, und dieser hat mit den Jahren der Entwicklung noch stetig abgenommen.

Eine grundlegende Aufgabe des Betriebssystems ist es, den auf dem System installierten Applikationen Zugriff auf die Funktionalitäten und Ressourcen zu bieten. Dies erfolgt über eine oder mehrere *Programmierschnittstellen* oder neudeutsch *application programming interface* (API). Diese – vom Hersteller des Betriebssystems festgelegten – Schnittstellen definieren die Art und den Umfang des Zugriffs der Applikationen auf die Daten und Funktionalitäten des Smartphones.

Problematisch ist der teils schwer kontrollierbare Datenfluss. So können bei bestimmten Betriebssystemumgebungen Applikationen z. B. auf das Telefonbuch zugreifen, ohne dass die Nutzerin oder der Nutzer davon Kenntnis hat oder diesen Zugriff unterbinden könnte. Derartige Zugriffsmöglichkeiten sind schlicht nicht akzeptabel. Gleiches gilt für den Zugriff auf Hardwareressourcen wie Speicher oder Kamera, der von einigen Applikationen eingefordert wird. Der Zugriff muss deutlich sichtbar und nachvollziehbar für Nutzende vom Betriebssystem geregelt werden und die nutzende Person muss sämtliche Berechtigungen jederzeit selbsttätig widerrufen können. Erfreulicherweise haben einige Hersteller in letzter Zeit insoweit die Information, Transparenz und Steuerungsmöglichkeiten für die Nutzerinnen und Nutzer verbessert.

Applikationen (Apps)

App hat sich als Kurzform für Applikation (engl. application), also eigentlich jede Art von Anwendungsprogramm, etabliert. Im deutschen Sprachgebrauch sind damit jedoch meist Anwendungen für Smartphones und Tablet-Computer gemeint, die mit einem für mobile Geräte ausgestatteten Betriebssystem betrieben werden. Typisch für diese spezielle Art von Applikationen ist, dass sie direkt aus dem Internet geladen und auf dem Endgerät installiert werden.

Die Hersteller der Betriebssysteme bieten auch Plattformen für den Vertrieb (und ggf. die Bezahlung) der Apps an, wobei unterschiedliche Regelungen für die Prüfung der Apps zum Tragen kommen. Teilweise ist es auch möglich, Apps unabhängig von der Vertriebsplattform zu installieren. Hier ist besondere Vorsicht angebracht und die

Quelle sollte wirklich vertrauenswürdig sein. Unabhängig von der Philosophie der Vermarktung dürfen die Grundsätze des Datenschutzes bei der Entwicklung nicht aus den Augen gelassen werden.

Die folgenden Aspekte sollten unter allen Umständen berücksichtigt werden:

- Transparenz gegenüber der nutzenden Person durch geeignete Dialoge,
- uneingeschränkte Kontrolle der Nutzenden über die Interaktion der Applikation mit den Ressourcen und Datenzugriff bzw. -speicherung nur nach Notwendigkeit,
- Aufklärung der Nutzerinnen und Nutzer schon vor der Installation der App, auf welche Ressourcen und Daten diese zugreifen wird – im Idealfall in einem kurzen und klaren Hinweis und nicht in seitenlangen juristischen Erläuterungen.

Updates

Nicht nur eine funktionierende IT-Ausstattung verlangt nach regelmäßigen und korrekten Updates, sondern auch die Betriebssysteme von Smartphones und die darauf installierten Apps sollten immer auf dem neuesten Stand sein. Wichtig ist hierbei, dass sowohl die Apps als auch das Betriebssystem regelmäßig geprüft werden und, sollten Updates verfügbar sein, diese auch zeitnah eingespielt werden.

Verantwortung der Nutzenden

Die Verantwortung für einen sicheren Betrieb des Endgerätes liegt ausschließlich bei der nutzenden Person. So sollten Sicherheitsupdates eingespielt werden und Apps nur von vertrauenswürdigen Quellen geladen werden. Zudem sollten die Datenschutzerklärungen aufmerksam gelesen werden und Anwendungen mit nicht plausiblen Zugriffen auf Ressourcen und Daten nicht installiert werden.

4.3 Mehrwertdienste

Mehrwertdienst ist ein Begriff, hinter dem sich in der Welt der Telekommunikation eine Menge von Diensten und Dienstleistungen verbirgt. Mehrwertdienste können dabei nicht allein an einer bestimmten Rufnummerngasse wie z. B. 0180 oder 0800 festgemacht werden.

Stellvertretend für die unzähligen denkbaren Dienstleistungen, die man unter diesem Begriff zusammenfassen kann, werden die bekanntesten Vertreter erläutert.

4.3.1 Servicenummern

Unter den kostenpflichtigen Servicenummern gibt es verschiedene Mehrwertdienste. Die bekanntesten sind kostenlose 0800-er Dienste („Free-Phone"), Service-Dienste („Shared-Cost"), die mit 0180 beginnen, die teureren 0900-er (ehemals 0190-er) „Premium-Rate"-Dienste und die sog. Massenverkehrs-Dienste, beginnend mit 0137.

Die kostenlosen Gespräche über eine 0800-er Rufnummer dürfen nicht auf dem Einzelverbindungsnachweis des anrufenden Anschlussinhabers aufgeführt werden, da diese nicht gebührenrelevant sind. In Einzelfällen waren diese in der Vergangenheit dort dennoch verzeichnet, was beispielsweise bei der Telefonseelsorge sehr bedenklich ist, die z. T. über kostenfreie 0800-er Nummern erreicht werden kann.

Bei den Premium-Rate- oder auch Service-Diensten kann man sich über aktuelle Börsenkurse oder Fußballergebnisse informieren, aber auch Telefonate jedes beliebigen Inhalts führen. Der Dienst selbst wird allerdings inhaltlich vom Anbieter gestaltet und ist ausschließlich von diesem zu verantworten. Durch 0900-er Rufnummern kann es zu sehr hohen Telefonrechnungen kommen, ebenso wie durch den übermäßigen Gebrauch der 0137-er Nummern, um sich bei Gewinnspielen im Vorteil zu wähnen. Die Kosten für Gewinnspielhotlines halten sich bei einmaligem Anruf mit wenigen Euro zwar noch in Grenzen, aber die 0900-er Familie ist meist frei zu tarifieren. Bei „Anruf in Abwesenheit" von einer 0900-er oder einer 0137-er Nummer kann es sich um einen teuren Rückruf bzw. um Betrug handeln.

Der Gesetzgeber hat, um dem Missbrauch teurer Rufnummerngassen vorzubeugen, in § 66i Absatz 3 TKG jeder nutzenden Person das Recht eingeräumt, von der BNetzA zu erfahren, welcher Anbieter sich hinter einer bestimmten Nummer verbirgt; nähere Informationen hierzu finden sich auf der Website (www.bundesnetzagentur.de).

4.3.2 Premium-SMS

Dienstleistungen zu ergänzen bzw. zusätzliche Produkte zu einem bestehenden Dienst hinzufügen, funktioniert heutzutage auch nonverbal. Man muss also nicht zwangsläufig sündhaft teure Nummern anrufen, denn die moderne Kommunikation erlaubt es auch, den Anbietern einen Text zu schreiben.
Premium-SMS können eingesetzt werden, um Zusatzleistungen (vorzugsweise in der Mobiltelefonie) zu buchen und zu bezahlen. Klingeltöne sind die bekanntesten Vertreter dieser Kategorie. Im Bezahlverfahren gibt es zwei unterschiedliche Methoden: Die Abrechnung erfolgt entweder pro geschriebener SMS des Nutzers oder pro empfangener SMS beim Anbieter.
Die Tarife für die einzelnen Nachrichten oder Abonnements sind vom Anbieter frei wählbar, werden unter den Mobilfunkanbietern abgestimmt und haben schon so manchen Teenager-Eltern beim Blick auf die Rechnung ein böses Erwachen beschert.

4.3.3 Gesprächsvermittlung

Auch die Vermittlung zweier Gesprächsteilnehmender durch einen Anbieter, der nicht der Anschlussinhaber ist, wird als Mehrwertdienst bezeichnet. Hierbei gibt es zwei Fälle, bei denen jeweils eine zusätzliche Erhebung und Speicherung von Verkehrsdaten, Identifikationsmerkmalen etc. erfolgt, die man dem Dienstleister zur Verfügung stellen muss. Grundsätzlich sollte sich jeder Nutzende vergegenwärtigen, wo und bei wem zusätzliche Daten erhoben werden; dies gilt auch für die Nutzung zur Verfügung gestellter Komfortfunktionen wie z. B. Online-Adressbücher.

Callback

Beim als *Callback* bezeichneten Dienst werden zwei Gesprächspartner von einem Dienstleister (der nicht der Netzbetreiber sein muss) per Rückruf (engl. callback) vermittelt, sprich: verbunden. Der Vorteil liegt in den geringeren Gebühren für ein Gespräch. Der Verbindungsaufbau ist hierbei untypisch: Einer der Gesprächspartner fordert entweder per SMS, Smartphone-App, Browser oder Anruf, bei dem sofort wieder aufgelegt wird, eine Verbindung der beiden Anschlüsse an, die daraufhin vom Dienstleister angerufen und verbunden werden.

Callthrough

Auch beim sog. *Callthrough* werden zwei Gesprächsteilnehmende durch einen Dienstleister verbunden. Im Unterschied zum Callback wählt sich hierbei jedoch der Anrufer in das System des Dienstleisters ein und gibt dort, häufig nach erfolgreicher Identifikation, die Rufnummer des zweiten Gesprächsteilnehmers an. Der Dienstleister baut auf einer zweiten Leitung eine Verbindung zu der gewünschten teilnehmenden Person auf und schaltet beide Beteiligte zusammen. Damit ist die Verbindung hergestellt und beide können wie gewohnt telefonieren. Callthrough ermöglicht es dem Anrufer, nach dem Vorbild des Call-by-Call, die Gesprächsgebühren zu senken. Der entscheidende Unterschied zum Call-by-Call ist jedoch, dass Callthrough nicht nur aus dem Festnetz möglich ist, sondern z. B. auch mit Mobiltelefonen vom Arbeitsplatz aus benutzt werden kann.

4.4 Rund um das Internet und die E-Mail

Die meisten Kundinnen und Kunden haben zusammen mit ihrem Telefonanschluss auch einen Zugang zum Internet gebucht; auch dabei handelt es sich um eine Telekommunikationsdienstleistung. Das Internet bietet zwar vielfältige Informationsmöglichkeiten, birgt aber auch Gefahren, beispielsweise Computerviren, Trojaner und nicht zuletzt die Möglichkeit, jede einzelne Person mit allerlei Werbung zu behelligen, ob gewollt oder nicht. Datenschutzrechtlich sind auch E-Mail-Dienste und andere Möglichkeiten zur direkten Kommunikation (etwa Instant Messaging) nach den Vorschriften des TKG zu bewerten; aufgrund technischer Gegebenheiten gibt es aber einige Besonderheiten.

4.4.1 Internetzugang

Neben den üblichen Bestandsdaten (s. Kapitel 2.5), die bei Vertragsschluss erhoben werden, sind für den Internet-Zugang die Nutzerkennung sowie ein Passwort erforderlich. Diese Daten dienen der Authentifizierung der Nutzenden bei der Einwahl ins Internet. Um im Internet surfen zu können, erhält die Nutzerin bzw. der Nutzer aus dem IP-Adressenbestand des Providers eine oder mehrere IP-Adressen, die an die Nutzerkennung gekoppelt sind. Auch IP-Adressen, die dynamisch vergeben werden, also prin-

zipiell von Einwahl zu Einwahl wechseln können, sind personenbezogene Daten, anhand derer die Anbieter die jeweiligen Kundinnen und Kunden identifizieren können.

Die Zuordnung, welche IP-Adresse eine Nutzerin oder ein Nutzer zu einem bestimmten Zeitpunkt erhalten hat, wird bei der dynamischen IP-Adressenvergabe in speziellen Logfiles gespeichert. Die BfDI hält es für zulässig, diese Daten für Datensicherheitszwecke bis zu sieben Tage zu speichern. Unter bestimmten Voraussetzungen können Strafverfolgungsbehörden die Herausgabe dieser Daten verlangen, um sie zur Ermittlung von Anschlüssen zu nutzen, soweit dies zur Verfolgung einer Straftat oder Ordnungswidrigkeit erforderlich ist (s. Kapitel 2.19 und 3.8). Auch bei vermuteten Urheberrechtsverletzungen wird ggf. auf diese Logfiles zurückgegriffen (s. Kapitel 3.7).

Zu den Verkehrsdaten zählen neben den IP-Adressen, Datum und Uhrzeit, das Volumen der übertragenen Daten und ggf. eine Anschlusskennung. Abhängig vom gewählten Tarif dürfen Verkehrsdaten für Abrechnungszwecke gespeichert werden. So ist bei einem Volumen-Tarif und einer Flatrate mit Drosselung die Speicherung von Nutzerkennung, Datenvolumen, Zeit und Dauer der Sitzung zur Ermittlung des Volumens erlaubt; bei einer sog. echten Flatrate entfällt die Kostenermittlung, so dass die Speicherung der Verkehrsdaten nicht zulässig ist.

Eine Sonderstellung im Bereich des Internetzugangs nehmen die sog. URLs ein, die landläufig auch als Surfdaten bezeichnet werden. Beim Surfen geben Nutzende in einem Browser eine bestimmte URL (Uniform Resource Locator) ein, die von einem DNS-Server in eine IP-Adresse umgesetzt wird. Auf diesem Wege wird der richtige Ort im Internet adressiert und die nutzende Person erhält die gewünschten Daten. URLs können Hinweise auf die Interessen und Vorlieben des jeweiligen Nutzenden geben, wie das Beispiel www.wetter-online.de/Frankreich/Paris.htm belegt. Oft reicht sogar die Angabe zu einer Website aus, z. B. www.bfdi.bund.de, um Rückschlüsse zu ziehen. Daher sind die URLs als besonders schützenswerte Inhaltsdaten anzusehen und dürfen vom Telekommunikationsanbieter nicht gespeichert werden.

Für Zwecke der Erkennung, Eingrenzung und Beseitigung von Störungen ermöglicht § 100 Absatz 1 TKG die Speicherung der Verkehrsdaten und von Steuerdaten informationstechnischer Protokolle, jedoch nicht von Inhaltsdaten. Ein Zeitraum von

höchstens sieben Tagen wird aufgrund langjähriger Erfahrung als ausreichend angesehen (s. Kapitel 2.10). Bei einer manuellen Erfassung oder Auswertung gibt es verschiedene Informationspflichten.

Weiterhin werden in § 109a Absatz 4 bis 6 TKG dem Netzbetreiber Maßnahmen zur Information des Nutzenden sowie Umleitung des Verkehrs oder Sperrung des Anschlusses erlaubt, um Störungen zu beseitigen, die von Systemen der jeweilig nutzenden Person ausgehen (s. Kapitel 2.17). Dies ist für Fälle gedacht, bei denen ein Gerät (z. B. PC) der Kundin oder des Kunden von Schadsoftware betroffen ist und andere Nutzende des Internets stört.

4.4.2 Internetnutzung in Hotels und Cafés

Betreiber von Hotels oder Cafés, die ihren Gästen einen Internetzugang anbieten, gelten nach § 3 Nr. 6 TKG als Diensteanbieter und unterliegen damit den Rechten und Pflichten des TKG (s. Kapitel 2.2). Gleiches gilt im Übrigen auch für öffentliche Stellen wie Behörden oder Krankenhäuser. Dies ist vielen Anbietern nicht bewusst. Dabei ist gerade die Einhaltung der datenschutzrechtlichen Vorgaben des TKG wichtig, denn der unzulässige Umgang mit Daten, die dem Fernmeldegeheimnis unterfallen, kann sogar einen Straftatbestand erfüllen. Eine gründliche Befassung mit den Rechten und Pflichten eines Telekommunikationsdiensteanbieters ist somit zwingend erforderlich.

Gerade – aber nicht ausschließlich – in Hotels müssen Gäste zur Nutzung des Internetangebotes oft verschiedene Angaben machen bzw. sich bereit erklären, dass beim Anbieter bereits vorhandene Daten im Zusammenhang mit der Erbringung des Internetzugangs verarbeitet werden dürfen. Sofern es sich hierbei um Bestandsdaten (s. Kapitel 2.5) handelt, bestehen hiergegen grundsätzlich keine Bedenken. Allerdings gilt – wie bei allen Diensteanbietern: Es dürfen nicht jedes abstrakt denkbare Datum, sondern nach § 95 Absatz 1 TKG nur solche Bestandsdaten erhoben werden, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste konkret erforderlich sind. Welche Daten dies sind, hängt in der Regel vom Einzelfall ab. Unabhängig davon sind sämtliche Bestandsdaten spätestens nach Ablauf der Frist des § 95 Absatz 3 TKG wieder zu löschen.

Die Speicherung und weitere Verarbeitung von Verkehrsdaten ist dagegen kritischer zu beurteilen (s. Kapitel 2.6). Sie ist zunächst nur erlaubt, wenn die Daten zur Abrechnung mit dem Nutzenden oder einem anderen Anbieter erforderlich sind. Bei kostenfreien Angeboten kann eine längerfristige Speicherung der anfallenden Verkehrsdaten somit nicht auf eine gesetzliche Grundlage gestützt werden.

In der Praxis besteht allerdings oftmals ein großes Interesse der Anbieter kostenloser öffentlich zugänglicher Internetzugängen, diese Daten weiterhin vorhalten zu können. Hierzu werden Logfiles der Zugangspunkte gespeichert, in denen detailliert protokolliert wird, wer zu welchem Zeitpunkt bestimmte Internetseiten angesurft hat. In Fällen der rechtsmissbräuchlichen Nutzung des Internetzugangs durch eine Nutzerin oder einen Nutzer kann so auch nachträglich belegt werden, wer genau den Rechtsverstoß begangen hat. Der Anbieter kann sich somit exkulpieren oder alternativ den verantwortlich Nutzenden in Regress nehmen. Problematisch ist jedoch, dass diese Logfiles neben Bestands- und Verkehrsdaten in der Regel noch weitere Informationen – vor allem die aufgerufenen URL – enthalten, die nicht gespeichert werden dürfen (s. Kapitel 4.4.1). Möchte ein Anbieter ungeachtet dessen eine entsprechende Datenverarbeitung vornehmen, ist er zwingend darauf angewiesen, sich im Vorhinein eine entsprechende Einwilligung (s. Kapitel 3.1) der Nutzerinnen und Nutzer einzuholen. Die an eine solche Einwilligung geknüpften Anforderungen sind aber aufgrund der Sensibilität der verarbeiteten Daten sehr hoch. So muss den Nutzenden (auch den Laien unter ihnen) beispielsweise klar und verständlich gemacht werden, welche ihrer Daten erfasst und für wie lange sie gespeichert werden. Diese wesentlichen Informationen müssen für sie unmittelbar zu erkennen sein, dürfen also nicht in allgemeinen Geschäfts- oder Nutzungsbedingungen versteckt werden. Ob und welche weiteren Besonderheiten noch zu beachten sind, hängt von den Umständen des Einzelfalls ab.

4.4.3 Internetprotokollversionen

IP-Adressen – kaum einer sieht sie und doch redet fast jeder davon. Das Internetprotokoll wird derzeit größtenteils noch in der Version 4 (IPv4) verwendet. Bei dieser Version kann durch die Begrenztheit noch von einer gewissen Anonymität der einzeln Nut-

zenden ausgegangen werden. Die knapp über vier Milliarden Adressen, die man in der „Kinderzeit“ des Internets reserviert hatte, reichen schon seit langem nicht mehr aus, alle Geräte anzubinden. Deshalb wurden Verfahren und Maßnahmen zur Vergabe von Adressen eingesetzt – insbesondere die sog. dynamische Vergabe von IP-Adressen -, die es ermöglichen, dass sich verschiedene Geräte und Nutzungsvorgänge eine IP-Adresse teilen. Dies hatte den aus Datenschutzsicht positiven Nebeneffekt, dass nicht die einzeln Nutzenden direkt anhand der IP-Adresse erkennbar sind.

Die Umstellung des Protokolls auf die Nachfolgerversion 6 (IPv6) mit einem wesentlich größeren Adressraum ist in Deutschland erfolgreich gestartet, so dass Schätzungen in 2018 von einem Marktanteil von bis zu 35 % ausgehen. Problematisch am neuen Protokoll ist: Mit der Erweiterung des Adressraumes ändert sich auch die grundlegende Strategie der Adressverteilung. Es ist mit IPv6 , jedes an das Internet angeschlossene Gerät mit einer eigenen dauerhaften IP-Adresse zu versehen, quasi eine Telefonnummer für jeden Computer, jede Kaffeemaschine und jeden Stromzähler. Angesichts dessen mögen sich jene schon die Hände reiben, deren Geschäfte auf der möglichst lückenlosen Registrierung des Nutzerverhaltens und der Bildung von Verhaltensprofilen basieren.

Deshalb lohnt es sich, das zugrundeliegende Verfahren näher zu betrachten. Was ist eigentlich ein Präfix und was macht dieses? Wozu dient der Interface Identifier und warum gibt es dafür kein deutsches Synonym?

Um die wichtigsten Fragen zu beantworten, soll zunächst der Aufbau der IPv6-Adresse genauer betrachtet werden: Eine IPv6-Adresse besteht aus zwei gleich großen Teilen, *Präfix* und *Interface Identifier* genannt. Die Länge der IPv6-Adresse bewirkt, dass eine nutzende Person grundsätzlich allein anhand des Präfix als auch allein durch den Interface Identifier eindeutig bestimmt werden kann. Deshalb sind für beide Teil-Adressen Vorkehrungen erforderlich, die diesem Identifizierungsrisiko begegnen.

Der vordere Teil, das sog. *Präfix,* wird vom Provider bestimmt und dem Anschluss des Nutzenden zugewiesen. Hier gibt es ähnlich wie beim „alten“ IPv4 unterschiedliche Arten der Zuweisung. Einem Anschluss kann entweder dauerhaft, also statisch, oder wechselnd, also dynamisch, ein Präfix zugeteilt werden. Die meisten Provider haben

sich für die dynamische Vergabe ausgesprochen, wenn auch der Auslöser für einen Wechsel variiert, nämlich zwischen Stecker aus der Steckdose ziehen und zeitlicher Begrenzungsvorgabe durch den Provider.

Der hintere Teil der Adresse, der sog. *Interface Identifier,* wird vom Endgerät des Nutzenden bestimmt. Da nicht nur das Präfix datenschutzrechtlich bedeutsam ist, sind auch hier Maßnahmen gefragt, die den Adressbestandteil veränderlich halten. Der (Quasi-) Standard zu IPv6 empfiehlt zu diesem Zweck den Einsatz der sog. *PrivacyExtensions.* Diese sorgen nicht nur dafür, dass die eineindeutige Hardwareadresse der Netzwerkkarte keinen unmittelbaren Eingang in die Adresse findet, sondern bewirken ferner einen regelmäßigen Wechsel der Netzwerkkartenkennung.

Jeder Nutzende, Geschäfts- oder Privatkunde sollte also genau hinsehen, wenn die Hochglanzprospekte der Anbieter von Diensten und Geräten eine völlig neue Welt versprechen. Genaues Nachfragen lohnt sich immer, besonders im Hinblick auf die Datenschutzmaßnahmen.

4.4.4 Voice over IP

Sprache wird heute grundsätzlich digital übertragen – bei einer guten Anbindung geht dies auch über das Internet. Bei VoIP sollte man sich bewusst sein, dass – ohne zusätzliche Sicherheitsmaßnahmen – die Vertraulichkeit der Kommunikation im Internet grundsätzlich nicht gewährleistet ist. Aufgrund seiner globalen Struktur können Datenpakete im Internet über viele Wege zum Ziel gelangen und ggf. sogar den Umweg über Server auf anderen Kontinenten nehmen. Deshalb darf nicht vergessen werden, dass im Ausland andere Regelungen für die Verarbeitung von Telekommunikationsdaten gelten als bei uns. So genießen Verkehrsdaten des Internet in den USA nicht den Schutz des deutschen Fernmeldegeheimnisses.

Telefonieren über das Internet kann preisgünstiger sein. Gespräche zwischen VoIP-Telefonen sind häufig sogar kostenlos und auch die Ortsanbindung entfällt. Ein VoIP-Telefon ist damit weltweit einsatzbereit und kann auch von bzw. zu einem Internetanschluss im Ausland genutzt werden. So kommen die allgemeinen Sicherheitsprobleme von

Datennetzen grundsätzlich auch bei der Internet-Telefonie zum Tragen. Dies gilt insbesondere für die Vertraulichkeit von Telefonaten, wenn bei VoIP Gesprächsinhalte unverschlüsselt über das Internet übertragen werden.

Eine Verschlüsselung ist zwar grundsätzlich möglich, wird aber nur bei bestimmten Diensten angeboten. Hier sind sowohl die Anbieter als auch die Hersteller von VoIP-Telefonen gefordert, datenschutzgerechte Lösungen einzusetzen. Wenn ein VoIP-Telefon direkt am heimischen DSL-Router angeschlossen wird, bedeutet dies zwar noch keine grundlegende Verschlechterung der Vertraulichkeit im Vergleich zum klassischen Telefon. Anders verhält es sich aber, wenn man im Urlaub das WLAN in seinem Hotel für Gespräche mit der Heimat nutzen will. Auch wenn der eigene Laptop mit einer VoIP- Software ausgestattet ist, sollte man sich gut überlegen, ob man vertrauliche Bankgeschäfte tätigt oder Gespräche mit seinem Arzt führt. Die Software zum Abhören von VoIP- Gesprächen ist leicht erhältlich. Ein VoIP-Endgerät ist ein kleiner Computer. Auch wenn dieser über Jahre funktioniert, sollte man regelmäßig die interne Betriebssoftware des Gerätes aktualisieren.

Ein spezielles Problem von VoIP betrifft die Rufnummernunterdrückung, die die Telekommunikationsunternehmen ihren Kundinnen und Kunden anbieten müssen. Für den Aufbau von VoIP-Verbindungen wird meist das Protokoll SIP genutzt. Bei Gesprächen zwischen Teilnehmenden besteht die Gefahr, dass die Rufnummernunterdrückung nicht oder nur unvollständig funktioniert. Unter Umständen kann sogar die gesamte von SIP übermittelte Protokollinformation angezeigt werden. Andererseits ist es für den Anrufer anhand der Rufnummer nicht erkennbar, ob der Angerufene einen normalen Telefonanschluss oder ebenfalls VoIP nutzt. Bei ankommenden Anrufen kann ggf. die im Endgerät angezeigte Rufnummer manipuliert werden. Dies führt zu Problemen, wenn man sich auf diese Nummer verlässt. Da diese Möglichkeiten von dem Server des Anbieters abhängen, sollte man sich bei ihm danach erkundigen, ob die Rufnummernunterdrückung funktioniert und ob die angezeigte Rufnummer bei ankommenden Gesprächen immer korrekt ist.

4.4.5 Wireless LAN (WLAN)

„Anytime, Anywhere“ ist das Stichwort für die mobile Kommunikation. Diese Vision ist Realität geworden: Die mobile Nutzung elektronischer Dienste ist heute gängige Praxis. Die Möglichkeiten gehen dabei weit über das einfache Telefonieren hinaus. Durch die drahtlose Kommunikationsinfrastruktur werden Komfort, Effizienz und Flexibilität verbessert. Arbeitsplätze können kurzfristig ohne kostenintensive Neuverkabelung eingerichtet werden. Mobile Arbeitskräfte wie z. B. Außendienstmitarbeiter können problemlos mit ihrem Notebook am Firmennetz teilnehmen, sobald sie in der Firma tätig sind.

Leider werden diese Vorteile oft durch einen Sicherheitsverlust für die via Funk übertragenen Daten und die Netze, an die die Funkkomponenten angeschlossen sind, erkauft. Zudem sind mobile Endgeräte und die darauf gespeicherten Daten einem hohen Verlust- und Diebstahlsrisiko ausgesetzt.

Funkwellen breiten sich prinzipiell unkontrolliert und unbegrenzt aus. Ist ein Gebäude komplett mit der Funkinfrastruktur ausgeleuchtet, so ist damit auch immer außerhalb des Gebäudes ein Empfang der Funkwellen möglich. Mitschnitte und Manipulationen der übertragenen Daten sind möglich, wenn keine Schutzmaßnahmen durchgeführt werden. Denial-of-Service-Attacken (DoS-Attacken) sind in ungeschützten Funknetzen relativ einfach durchführbar, ebenso wie Man-in-the-middle-Attacken, bei denen durch geschickte Positionierung von Funkkomponenten echte Gegenstellen vorgegaukelt werden und dadurch z. B. die Datenübertragung zu bestimmten Netz-Segmenten protokolliert oder blockiert werden kann.

Große Sicherheitsrisiken bestehen bereits, wenn Geräte „Out-Of-The-Box“ eingesetzt werden, die ohne Anpassung der Konfiguration und mit „Default“-Passwörtern arbeiten. Wer sich auf die eingebauten Sicherheitsmechanismen verlässt, ist oft nicht sicher. Glücklicherweise unterstützen die gängigen WLAN-Komponenten das Wi-Fi Protected Access 2 (WPA2)-Verfahren, das im Standard zu WLAN festgeschriebene Verschlüsselungsverfahren, das in der Voreinstellung der meisten Access-Points und WLAN-Karten oftmals bereits aktiviert ist. Somit kann unter den drahtlosen Geräten ein gewisses Maß an Sicherheit garantiert werden, auch wenn diese Art des Schutzes immer

mit einem Administrationsaufwand für den Besitzer einhergeht. Die WEP-Verschlüsselung und möglichst auch die WPA-Verschlüsselung sollten nicht mehr verwendet werden.

Öffentliche WLAN-Hot-Spots, wie zum Beispiel an Flughäfen oder Bahnhöfen, nehmen unter den Drahtlosnetzwerken einen Sonderstatus ein. Hot-Spots verfügen oft nicht über ein Verschlüsselungsverfahren als Schutz gegen unbefugten Zugang und Abhören und bieten somit jedem den Zugriff auf das drahtlose Netzwerk und alle darin vorhandenen Daten.

Dementsprechend ist jeder Nutzende für die eigene Sicherheit verantwortlich und sollte dafür sorgen, dass der Datenverkehr unversehrt bleibt. Die Vergangenheit hat gezeigt, dass gerade solche Umgebungen der ideale Ausgangspunkt für Angriffe auf E-Mails, Chats und Telefongespräche übers Internet sind. Unverschlüsselte Verbindungen oder Pakete können leicht abgefangen werden, ohne dass Absender oder Empfänger etwas davon mitbekommen und die Entzifferung des Inhaltes ist meist ein Leichtes. Die Verwendung eines verschlüsselten Kanals (VPN) für alle Anwendungen bzw. einzelner verschlüsselter Verbindungen (https, SSL/TLS) sollte deswegen obligatorisch sein.

Zudem speichern einige gewerbliche Betreiber öffentlicher Hot-Spots Verkehrs- und Bestandsdaten, um ggf. kostenpflichtige Leistungen gegenüber dem Nutzer abzurechnen. Dies sollte jedem Nutzer bewusst sein, der einen solchen Dienst in Anspruch nimmt; nicht alle Betreiber ermöglichen ein anonymes Surf-Vergnügen.

4.5 E-Mail

Mit dem Zugang zum Internet erhalten Kundinnen und Kunden eines Telekommunikationsanbieters auch einen E-Mail-Account, so dass sich die zugeordneten Bestandsdaten um die E-Mail-Adresse und das Passwort erweitern. Anders als bei vielen kostenfreien Webmailangeboten verfügt der Telekommunikationsanbieter in jedem Fall über die korrekten Bestandsdaten zu dem E-Mail-Account seiner Kundinnen und Kunden, die er für Auskünfte gemäß §§ 111 und 112 TKG speichern muss (s. Kapitel 2.19 und 2.20).

Die E-Mail-Provider erheben teils umfangreiche Bestandsdaten. Auf den ersten Blick erscheint dies zumindest bei den kostenfreien Tarifen nicht erforderlich, wird aber nachvollziehbar mit den Pflichten des Providers begründet, z. B. bei Haftungsfragen und namensrechtlichen Problemen. Die E-Mail-Adresse ist im Rahmen der Verfügbarkeit vom Nutzenden frei wählbar, d. h. es besteht die Möglichkeit, die Nachrichten unter einem Pseudonym zu versenden. Vielfach werden die von den Nutzerinnen und Nutzern angegebenen Daten aber nicht verifiziert, sondern nur auf Plausibilität überprüft. Bank- und Kreditkartendaten darf der Anbieter nur dann erheben, wenn Nutzende sich für einen kostenpflichtigen Tarif angemeldet oder vom kostenfreien in einen kostenpflichtigen gewechselt haben.

Da die kostenfreien Tarife werbefinanziert sind, werden Nutzende animiert, zusätzlich Angaben zu Interessen und Hobbys zu machen, damit die passende Werbung eingeblendet werden kann. Oftmals wird auch regelmäßig ein Newsletter versandt, den die Kundin bzw. der Kunde im Freemail-Tarif nicht abbestellen kann und der neben Informationen zu Produktneuheiten auch verschiedene Werbebotschaften enthält. Dieses Vorgehen ist akzeptabel, wenn ein zwar kostenpflichtiger, aber gleichwertiger Tarif angeboten wird.

Der Widerspruch gegen die Zusendung eines Newsletters mit eigenen Angeboten des Providers muss jedenfalls bei einem kostenpflichtigen Angebot möglich sein, ebenso ein völlig werbefreier E-Mail-Account. Will der Provider auch fremde Werbung versenden, benötigt er die Einwilligung seiner Kundinnen und Kunden. E-Mail-Provider sind nicht verpflichtet, Bestandsdaten eigens für Auskunftsersuchen der Sicherheitsbehörden zu erheben und zu speichern, sondern müssen diese Daten nur dann für die genannten Zwecke bereithalten, wenn sie diese sowieso für ihre eigenen Zwecke speichern.

Die beim E-Mail-Verkehr anfallenden Verkehrsdaten werden nicht für Abrechnungszwecke benötigt – E-Mails werden üblicherweise nicht abgerechnet – und dürfen somit nicht gespeichert werden. Allerdings ist eine Speicherung für Datensicherheitszwecke für einen begrenzten Zeitraum zulässig, z. B. zum Erkennen und zur Abwehr von Spam-Angriffen. Hier können höchstens sieben Tage als angemessen gelten. Bei entgeltpflichtigen Diensten, z. B. E-Mail to SMS, kann eine Speicherung jedoch erforderlich sein. Da das Aufkommen unerwünschter Werbemails (Spam) immer mehr zugenommen

hat und durch Spam-Mails auch Viren und Trojaner verbreitet und leichtsinnige Nutzer auf Abzockseiten geleitet werden, setzten die E-Mail-Provider an ihren Gateways Spam-Filter und Virenscanner ein. Durch den Einsatz von Blacklists (Listen von Servern, von denen bekanntermaßen Spams versendet werden) und durch das sog. Greylisting, bei dem E-Mails von unbekannten Absendern erst nach einem erneuten Melden des absendenden (guten) Servers angenommen werden, können die meisten Spam-Mails abgewiesen werden. Zusätzlich bieten die E-Mail-Provider Spam-Filter für das Postfach des Nutzers an, die er selbst aktivieren und konfigurieren kann.

Die Virenscanner überprüfen die Inhalte ein- und ausgehender E-Mails auf verdächtigen Schadcode. Dies geschieht automatisiert und anhand von sog. Viren-Signaturen. Wird ein Virus erkannt, wird er entfernt und die E-Mail ohne den Schadcode und mit einer entsprechenden Mitteilung dem Empfänger zugestellt. Die verseuchte E-Mail wird auf einem Quarantäne-Server zur weiteren Analyse vorgehalten.

Die Verwendung der Verkehrsdaten und das automatisierte Prüfen der E-Mail-Inhalte auf Schadcode sind zulässig; der Provider kann sich zum Schutz der technischen Systeme im dafür erforderlichen Maß Kenntnis vom Inhalt und den Umständen der Telekommunikation verschaffen (§ 88 Absatz 3 Satz 1 TKG).

4.6 Messenger-Dienste

Instant Messaging (englisch: “augenblickliche Nachrichtenübermittlung”) ermöglicht es nahezu in Echtzeit, Textnachrichten zwischen den Teilnehmenden desselben Messenger-Dienstes zu versenden und zu erhalten. Dabei erscheinen die Nachrichten sofort auf dem Bildschirm des anderen und können von diesem auch umgehend beantwortet werden. Neben reinen Textmitteilungen können auch Dateien aller Art (Fotos, Video- u. Audiofiles, Word-Dokumente etc.) versendet werden. Benötigt wird eine Software (App), die auf dem Endgerät (Smartphone, Tablet oder PC) installiert werden muss. Auch soziale Netzwerke integrierten in den letzten Jahren Instant-Messaging-Systeme. Bekannte Beispiele sind Snapchat, WhatsApp oder der Facebook-Messenger.

Datenschutzrechtlich relevant sind dabei insbesondere die Daten, die man zur Nutzung bereitstellen muss, die Zugriffsrechte, z. B. auf Kontaktlisten, die dem Messenger-Dienst eingeräumt werden müssen sowie die Konfigurationsmöglichkeiten zur Kennzeichnung von öffentlichen und privaten Informationen. Die Anwendungen unterscheiden sich auch in der Möglichkeit, Audits z. B. zur eingesetzten Verschlüsselung durchzuführen oder die Lebensdauer der Nachrichten einzuschränken.

Das TKG stammt aus einer Zeit, in der ausschließlich klassische Telekommunikationsanbieter Dienste angeboten haben. Heute ersetzen die Messenger-Dienste jedoch zunehmend die klassische Telefonie. Messenger-Dienste als Over-The-Top (OTT)-Kommunikationsdienst, die eine Kommunikation über Internetzugänge ermöglichen, ohne dass ein Internetdiensteanbieter in die Kontrolle oder Verbreitung der Inhalte involviert ist, stehen als solche in einer Konkurrenzbeziehung zum klassischen Telekommunikationsdienst (TK-Dienst) wie SMS oder Sprachtelefonie. Daher sind diese rechtlich wie ein „klassischer" TK-Dienst zu behandeln und unterfallen dem TKG. Auch sieht im Rahmen der Überarbeitung der E-Privacy-Richtlinie die Nachfolgeregelung die Inklusion der OTT-Dienste vor. Bislang fühlen sich aber vor allem ausländische Messenger-Dienste-Anbieter bis zum In-Kraft-treten der Nachfolgeregelung zur E-Privacy-Richtlinie, also der E-Privacy-Verordnung, jedoch weder dem TMG noch dem TKG verpflichtet.

Auf europäischer Ebene konnte jedoch ein wichtiger Erfolg zum Schutz der personenbezogenen Daten im Zusammenhang mit einem weitverbreiteten Messenger-Dienst erzielt werden. Mit der Übernahme der WhatsApp Inc. durch Facebook hatte WhatsApp im August 2015 eine Aktualisierung ihrer Nutzungsbedingungen und Datenschutzbestimmungen angekündigt. Danach sollte einer Weitergabe von Daten innerhalb der "Facebook-Unternehmensgruppe" zu Zwecken, die in den Nutzungsbedingungen und der Datenschutzrichtlinie nicht enthalten waren, durch bestehende Nutzer zugestimmt werden, andernfalls könne der Dienst nicht weitergenutzt werden. Am 27. Oktober 2016 hat die Artikel-29-Gruppe in einem Schreiben bezüglich der Weitergabe von Informationen innerhalb der "Facebook-Unternehmensgruppe" Bedenken zur Gültigkeit der Einwilligung der Nutzer und der Rechte von Nicht-Facebook-Nutzern im Hinblick auf die angekündigte Änderung der Datenschutzrichtlinie geäußert. Daher forderte die Artikel-29-Gruppe WhatsApp Inc. auf, alle relevanten Informationen so bald wie mög-

lich der Artikel-29-Gruppe zur Verfügung zu stellen. Auch wurde das Unternehmen aufgefordert, den konzernweiten Austausch von WhatsApp Nutzerdaten zu unterbrechen, bis ein angemessener rechtlicher Schutz für die betroffenen Personen gewährleistet wird. Immerhin wurde die Übermittlung von WhatsApp-Nutzerdaten an Facebook zu Werbezwecken darauf hin EU-weit von der WhatsApp Inc. bis heute nicht umgesetzt. Die Gespräche zu diesem Themenkomplex dauern zur Drucklegung dieser Auflage noch an.

4.7 Gesprächsaufzeichnung und Mithören

Gesprächsaufzeichnung

Viele Unternehmen, auch Telekommunikationsdiensteanbieter, zeichnen Telefonate mit Kunden auf. Sie begründen dies überwiegend mit der Verbesserung ihrer Servicequalität, es erfolgen aber auch Aufzeichnungen zu Dokumentationszwecken z. B. im Zusammenhang mit Vertragsabschlüssen, die telefonisch getätigt werden.

Gespräche dürfen grundsätzlich nur dann aufgezeichnet werden, wenn der Anrufer der Aufzeichnung vorher zustimmt. Wer eine Gesprächsaufzeichnung unbefugt fertigt, verletzt die Vertraulichkeit des Wortes und begeht eine Straftat (§ 201 StGB), die aber nur auf Antrag verfolgt wird. Eine Gesprächsaufzeichnung ist nur dann zulässig, wenn die Einwilligung von Anrufenden über die Tastatur oder über die Sprachsteuerung vor Aufzeichnungsbeginn per Zustimmung von Betroffenen eingeholt wird (sog. Opt-In-Verfahren).

Die von den Unternehmen dabei eingesetzten Verfahren geben immer wieder Anlass zu Kritik. Ein Grund hierfür ist, dass die Aufzeichnungspraxis unterschiedlich gehandhabt wird. Die BfDI strebt deshalb eine einheitliche Vorgehensweise bei den Callcentern an, die direkt von den Telekommunikationsdiensteanbietern betrieben werden. Die Einwilligung der Kundinnen und Kunden soll ausdrücklich vor dem eigentlichen Telefonat eingeholt werden. Hierzu gibt es bereits positive Beispiele, in denen die Einwilligung über die Tastatur oder über die Sprachsteuerung vor Gesprächsbeginn erteilt wird. Die Telekommunikationsdiensteanbieter signalisieren erfreulicherweise, künftig diese Ein-

willigungslösung einzusetzen. Es ist deshalb davon auszugehen, dass sich die Problematik in absehbarer Zeit erledigen wird, wobei den Unternehmen ein gewisser Zeitrahmen für die Umstellung eingeräumt wird.

Bei einem Vertragsabschluss am Telefon dokumentieren Call-Center-Beschäftigte das Einverständnis durch eine Gesprächsaufzeichnung. Dies dient der Sicherheit, falls es nach Zusendung der schriftlichen Auftragsbestätigung zu Unstimmigkeiten kommen sollte. Eine Aufzeichnung darf natürlich auch hier nur mit der ausdrücklichen Zustimmung des Anrufers erfolgen.

Mithören

Oft hören Dritte über eingebaute Lautsprecher oder Zweithörer Telefongespräche mit, um z. B. bei Streitigkeiten später als Zeuge präsentiert werden zu können.

Das BVerfG hat in seinem am 31. Oktober 2002 veröffentlichten Beschluss über zwei Verfassungsbeschwerden entschieden, dass das Mithören unzulässig ist, wenn der andere Telefongesprächspartner nicht zuvor eingewilligt hat. Die Einwilligung braucht allerdings nicht ausdrücklich erklärt zu werden, sondern kann sich auch aus den Umständen ergeben.

Das Fernmeldegeheimnis gemäß Artikel 10 Absatz 1 GG schützt nur davor, dass niemand die Telefonleitung anzapft. Wie das BVerfG hierzu dagegen festgestellt hat, verletzt das unerlaubte Mithören das Recht am gesprochenen Wort. Dieses Recht ist Teil des Persönlichkeitsrechts eines Jeden (Artikel 2 Absatz 1 i. V .m. Artikel 1 Absatz 1 GG). Der Gesetzgeber hat es bis heute versäumt, dem konkret Rechnung zu tragen. Die Beschäftigten in Behörden und Unternehmen sollten aber angewiesen werden, das Einschalten einer Mithöreinrichtung stets von der Einwilligung ihres Telefongesprächspartners abhängig zu machen.

Übersicht Anhänge

Anhang 1

Telekommunikationsgesetz – auszugsweise –

Zum 11. Januar 2018 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: Zuletzt geändert durch Art. 22 Abs. 3 G v. 23.6.2017 | 1822

Hinweis: Änderung durch Art. 5 G v. 23.6.2017 | 1885 (Nr. 40) mWv 30.6.2017 durch juris textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

Änderung durch Art. 2 G v. 27.6.2017 | 1947 (Nr. 42) mWv 4.7.2017 textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

Änderung durch Art. 1 G v. 27.6.2017 | 1963 (Nr. 42) mWv 4.7.2017 textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

Änderung durch Art. 10 Abs. 12 G v. 30.10.2017 | 3618 mWv 9.11.2017 (Nr. 71) textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

Teil 1 Allgemeine Vorschriften

§ 1 Zweck des Gesetzes

Zweck dieses Gesetzes ist es, durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten.

§ 2 Regulierung, Ziele und Grundsätze

(1) Die Regulierung der Telekommunikation ist eine hoheitliche Aufgabe des Bundes.

(2) Ziele der Regulierung sind:

1. die Wahrung der Nutzer-, insbesondere der Verbraucherinteressen auf dem Gebiet der Telekommunikation und die Wahrung des Fernmeldegeheimnisses. Die Bundesnetzagentur fördert die Möglichkeit der Endnutzer, Informationen abzurufen und zu verbreiten oder Anwendungen und Dienste ihrer Wahl zu nutzen. Die Bundesnetzagentur berücksichtigt die Bedürfnisse bestimmter gesellschaftlicher Gruppen, insbesondere von behinderten Nutzern, älteren Menschen und Personen mit besonderen sozialen Bedürfnissen,

2. die Sicherstellung eines chancengleichen Wettbewerbs und die Förderung nachhaltig wettbewerbsorientierter Märkte der Telekommunikation im Bereich der Telekommunikationsdienste und -netze sowie der zugehörigen Einrichtungen und Dienste, auch in der Fläche. Die Bundesnetzagentur stellt insoweit auch sicher, dass für die Nutzer, einschließlich be-

hinderter Nutzer, älterer Menschen und Personen mit besonderen sozialen Bedürfnissen, der größtmögliche Nutzen in Bezug auf Auswahl, Preise und Qualität erbracht wird. Sie gewährleistet, dass es im Bereich der Telekommunikation, einschließlich der Bereitstellung von Inhalten, keine Wettbewerbsverzerrungen oder -beschränkungen gibt,

3. die Entwicklung des Binnenmarktes der Europäischen Union zu fördern,

4. die Sicherstellung einer flächendeckenden gleichartigen Grundversorgung in städtischen und ländlichen Räumen mit Telekommunikationsdiensten (Universaldienstleistungen) zu erschwinglichen Preisen,

5. die Beschleunigung des Ausbaus von hochleistungsfähigen öffentlichen Telekommunikationsnetzen der nächsten Generation,

6. die Förderung von Telekommunikationsdiensten bei öffentlichen Einrichtungen,

7. die Sicherstellung einer effizienten und störungsfreien Nutzung von Frequenzen, auch unter Berücksichtigung der Belange des Rundfunks,

8. eine effiziente Nutzung von Nummerierungsressourcen zu gewährleisten,

9. die Wahrung der Interessen der öffentlichen Sicherheit.

(3) Die Bundesnetzagentur wendet bei der Verfolgung der in Absatz 2 festgelegten Ziele objektive, transparente, nicht diskriminierende und verhältnismäßige Regulierungsgrundsätze an, indem sie unter anderem

1. die Vorhersehbarkeit der Regulierung dadurch fördert, dass sie über angemessene Überprüfungszeiträume ein einheitliches Regulierungskonzept beibehält,

2. gewährleistet, dass Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten unter vergleichbaren Umständen nicht diskriminiert werden,

3. den Wettbewerb zum Nutzen der Verbraucher schützt und, soweit sachgerecht, den infrastrukturbasierten Wettbewerb fördert,

4. effiziente Investitionen und Innovationen im Bereich neuer und verbesserter Infrastrukturen auch dadurch fördert, dass sie dafür sorgt, dass bei jeglicher Zugangsverpflichtung dem Risiko der investierenden Unternehmen gebührend Rechnung getragen wird, und dass sie verschiedene Kooperationsvereinbarungen zur Aufteilung des Investitionsrisikos zwischen Investoren und Zugangsbegehrenden zulässt, während sie gleichzeitig gewährleistet, dass der Wettbewerb auf dem Markt und der Grundsatz der Nichtdiskriminierung gewahrt werden,

5. die vielfältigen Bedingungen im Zusammenhang mit Wettbewerb und Verbrauchern, die in den verschiedenen geografischen Gebieten innerhalb der Bundesrepublik Deutschland herrschen, gebührend berücksichtigt und

6. regulatorische Vorabverpflichtungen nur dann auferlegt, wenn es keinen wirksamen und nachhaltigen Wettbewerb gibt, und diese Verpflichtungen lockert oder aufhebt, sobald es einen solchen Wettbewerb gibt.

(4) Die Vorschriften des Gesetzes gegen Wettbewerbsbeschränkungen bleiben, soweit nicht durch dieses Gesetz ausdrücklich abschließende Regelungen getroffen werden, anwendbar. Die Aufgaben und Zuständigkeiten der Kartellbehörden bleiben unberührt.

(5) Die hoheitlichen Rechte des Bundesministeriums der Verteidigung bleiben unberührt.

(6) Die Belange des Rundfunks und vergleichbarer Telemedien sind unabhängig von der Art der Übertragung zu berücksichtigen. Die medienrechtlichen Bestimmungen der Länder bleiben unberührt.

§ 3 Begriffsbestimmungen

Im Sinne dieses Gesetzes ist oder sind

1. „Anruf" eine über einen öffentlich zugänglichen Telekommunikationsdienst aufgebaute Verbindung, die eine zweiseitige Sprachkommunikation ermöglicht;

2. „Anwendungs-Programmierschnittstelle" die Software-Schnittstelle zwischen Anwendungen, die von Sendeanstalten oder Diensteanbietern zur Verfügung gestellt werden, und den Anschlüssen in den erweiterten digitalen Fernsehempfangsgeräten für digitale Fernseh- und Rundfunkdienste;

2a. „Auskunftsdienste" bundesweit jederzeit telefonisch erreichbare Dienste, insbesondere des Rufnummernbereichs 118, die ausschließlich der neutralen Weitergabe von Rufnummer, Name, Anschrift sowie zusätzlichen Angaben von Telekommunikationsnutzern dienen. Die Weitervermittlung zu einem erfragten Teilnehmer oder Dienst kann Bestandteil des Auskunftsdienstes sein;

2b. „Baudenkmäler" nach Landesrecht geschützte Gebäude oder Gebäudemehrheiten;

3. „Bestandsdaten" Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden;

4. „beträchtliche Marktmacht" eines oder mehrerer Unternehmen gegeben, wenn die Voraussetzungen nach § 11 Absatz 1 Satz 3 und 4 vorliegen;

4a. „Betreiberauswahl" der Zugang eines Teilnehmers zu den Diensten aller unmittelbar zusammengeschalteten Anbieter von öffentlich zugänglichen Telekommunikationsdiensten im Einzelwahlverfahren durch Wählen einer Kennzahl;

4b. „Betreibervorauswahl“ der Zugang eines Teilnehmers zu den Diensten aller unmittelbar zusammengeschalteten Anbieter von öffentlich zugänglichen Telekommunikationsdiensten durch festgelegte Vorauswahl, wobei der Teilnehmer unterschiedliche Voreinstellungen für Orts- und Fernverbindungen vornehmen kann und bei jedem Anruf die festgelegte Vorauswahl durch Wählen einer Betreiberkennzahl übergehen kann;

5. „Dienst mit Zusatznutzen” jeder Dienst, der die Erhebung und Verwendung von Verkehrsdaten oder Standortdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Entgeltabrechnung dieses Vorganges erforderliche Maß hinausgeht;

6. „Diensteanbieter” jeder, der ganz oder teilweise geschäftsmäßig

   a) Telekommunikationsdienste erbringt oder

   b) an der Erbringung solcher Dienste mitwirkt;

7. „digitales Fernsehempfangsgerät” ein Fernsehgerät mit integriertem digitalem Decoder oder ein an ein Fernsehgerät anschließbarer digitaler Decoder zur Nutzung digital übertragener Fernsehsignale, die mit Zusatzsignalen, einschließlich einer Zugangsberechtigung, angereichert sein können;

7a. „digitales Hochgeschwindigkeitsnetz“ ein Telekommunikationsnetz, das die Möglichkeit bietet, Datendienste mit Geschwindigkeiten von mindestens 50 Megabit pro Sekunde bereitzustellen;

7b. „Einzelrichtlinien“

   a) die Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie) (ABl. L 108 vom 24.4.2002, S. 21), die zuletzt durch die Richtlinie 2009/140/EG (ABl. L 337 vom 18.12.2009, S. 37) geändert worden ist;

   b) die Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie) (ABl. L 108 vom 24.4.2002, S. 7), die zuletzt durch die Richtlinie 2009/140/EG (ABl. L 337 vom 18.12.2009, S. 37) geändert worden ist;

   c) die Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie) (ABl. L 108 vom 24.4.2002, S. 51), die zuletzt durch die Richtlinie 2009/136/EG (ABl. L 337 vom 18.12.2009, S. 11) geändert worden ist;

   d) die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der

elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37), die zuletzt durch die Richtlinie 2009/136/EG (ABl. L 337 vom 18.12.2009, S. 11) geändert worden ist, und

e) die Richtlinie 2014/61/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Maßnahmen zur Reduzierung der Kosten des Ausbaus von Hochgeschwindigkeitsnetzen für die elektronische Kommunikation (Kostensenkungsrichtlinie) (ABl. L 155 vom 23.5.2014, S. 1);

8. „Endnutzer“ ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt;

8a. „entgeltfreie Telefondienste” Dienste, insbesondere des Rufnummernbereichs (0)800, bei deren Inanspruchnahme der Anrufende kein Entgelt zu entrichten hat;

8b. „Service-Dienste” Dienste, insbesondere des Rufnummernbereichs (0)180, die bundesweit zu einem einheitlichen Entgelt zu erreichen sind;

9. „Frequenznutzung” jede gewollte Aussendung oder Abstrahlung elektromagnetischer Wellen zwischen 9 kHz und 3 000 GHz zur Nutzung durch Funkdienste und andere Anwendungen elektromagnetischer Wellen;

9a. „Frequenzzuweisung“ die Benennung eines bestimmten Frequenzbereichs für die Nutzung durch einen oder mehrere Funkdienste oder durch andere Anwendungen elektromagnetischer Wellen, falls erforderlich mit weiteren Festlegungen;

9b. „gemeinsamer Zugang zum Teilnehmeranschluss“ die Bereitstellung des Zugangs zum Teilnehmeranschluss oder zum Teilabschnitt in der Weise, dass die Nutzung eines bestimmten Teils der Kapazität der Netzinfrastruktur, wie etwa eines Teils der Frequenz oder Gleichwertiges, ermöglicht wird;

9c. „GEREK“ das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation;

9d. „Gerät“ eine Funkanlage, eine Telekommunikationsendeinrichtung oder eine Kombination von beiden;

10. „geschäftsmäßiges Erbringen von Telekommunikationsdiensten” das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht;

10a. (weggefallen)

11. „Kundenkarten” Karten, mit deren Hilfe Telekommunikationsverbindungen hergestellt und personenbezogene Daten erhoben werden können;

11a. „Kurzwahl-Datendienste” Kurzwahldienste, die der Übermittlung von nichtsprachgestützten Inhalten mittels Telekommunikation dienen und die keine Telemedien sind;

11b. „Kurzwahldienste" Dienste, die die Merkmale eines Premium-Dienstes haben, jedoch eine spezielle Nummernart mit kurzen Nummern nutzen;

11c. „Kurzwahl-Sprachdienste" Kurzwahldienste, bei denen die Kommunikation sprachgestützt erfolgt;

11d. „Massenverkehrs-Dienste" Dienste, insbesondere des Rufnummernbereichs (0)137, die charakterisiert sind durch ein hohes Verkehrsaufkommen in einem oder mehreren kurzen Zeitintervallen mit kurzer Belegungsdauer zu einem Ziel mit begrenzter Abfragekapazität;

12. „nachhaltig wettbewerbsorientierter Markt" ein Markt, auf dem der Wettbewerb so abgesichert ist, dass er ohne sektorspezifische Regulierung besteht;

12a. „Netzabschlusspunkt" der physische Punkt, an dem einem Teilnehmer der Zugang zu einem Telekommunikationsnetz bereitgestellt wird; in Netzen, in denen eine Vermittlung oder Leitwegebestimmung erfolgt, wird der Netzabschlusspunkt anhand einer bestimmten Netzadresse bezeichnet, die mit der Nummer oder dem Namen eines Teilnehmers verknüpft sein kann;

12b. „Neuartige Dienste" Dienste, insbesondere des Rufnummernbereichs (0)12, bei denen Nummern für einen Zweck verwendet werden, für den kein anderer Rufnummernraum zur Verfügung steht;

13. „Nummern" Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen;

13a. „Nummernart" die Gesamtheit aller Nummern eines Nummernraums für einen bestimmten Dienst oder eine bestimmte technische Adressierung;

13b. „Nummernbereich" eine für eine Nummernart bereitgestellte Teilmenge des Nummernraums;

13c. „Nummernraum" die Gesamtheit aller Nummern, die für eine bestimmte Art der Adressierung verwendet werden;

13d. „Nummernteilbereich" eine Teilmenge eines Nummernbereichs;

14. „Nutzer" jede natürliche oder juristische Person, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt oder beantragt, ohne notwendigerweise Teilnehmer zu sein;

15. „öffentliches Münz- und Kartentelefon" ein der Allgemeinheit zur Verfügung stehendes Telefon, für dessen Nutzung als Zahlungsmittel unter anderem Münzen, Kredit- und Abbuchungskarten oder Guthabenkarten, auch solche mit Einwahlcode, verwendet werden können;

16. „öffentliches Telefonnetz" ein Telekommunikationsnetz, das zur Bereitstellung des öffentlich zugänglichen Telefondienstes genutzt wird und darüber hinaus weitere Dienste wie Telefax- oder Datenfernübertragung und einen funktionalen Internetzugang ermöglicht;

16a. „öffentliches Telekommunikationsnetz" ein Telekommunikationsnetz, das ganz oder überwiegend der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen;

16b. „öffentliche Versorgungsnetze" entstehende, betriebene oder stillgelegte physische Infrastrukturen für die öffentliche Bereitstellung von

a) Erzeugungs-, Leitungs- oder Verteilungsdiensten für

aa) Telekommunikation,

bb) Gas,

cc) Elektrizität, einschließlich der Elektrizität für die öffentliche Straßenbeleuchtung,

dd) Fernwärme oder

ee) Wasser, ausgenommen Trinkwasser im Sinne des § 3 Nummer 1 der Trinkwasserverordnung in der Fassung der Bekanntmachung vom 10. März 2016 (BGBl. | S. 459), die durch Artikel 4 Absatz 21 des Gesetzes vom 18. Juli 2016 (BGBl. | S. 1666) geändert worden ist; zu den öffentlichen Versorgungsnetzen zählen auch physische Infrastrukturen zur Abwasserbehandlung und -entsorgung sowie die Kanalisationssysteme;

b) Verkehrsdiensten; zu diesen Infrastrukturen gehören insbesondere Schienenwege, Straßen, Wasserstraßen, Brücken, Häfen und Flugplätze;

17. „öffentlich zugänglicher Telefondienst" ein der Öffentlichkeit zur Verfügung stehender Dienst, der direkt oder indirekt über eine oder mehrere Nummern eines nationalen oder internationalen Telefonnummernplans oder eines anderen Adressierungsschemas das Führen folgender Gespräche ermöglicht:

a) aus- und eingehende Inlandsgespräche oder

b) aus- und eingehende Inlands- und Auslandsgespräche;

17a. „öffentlich zugängliche Telekommunikationsdienste" der Öffentlichkeit zur Verfügung stehende Telekommunikationsdienste;

17b. „passive Netzinfrastrukturen" Komponenten eines Netzes, die andere Netzkomponenten aufnehmen sollen, selbst jedoch nicht zu aktiven Netzkomponenten werden; hierzu zählen zum Beispiel Fernleitungen, Leer- und Leitungsrohre, Kabelkanäle, Kontrollkammern, Ein-

stiegsschächte, Verteilerkästen, Gebäude und Gebäudeeingänge, Antennenanlagen und Trägerstrukturen wie Türme, Ampeln und Straßenlaternen, Masten und Pfähle; Kabel, einschließlich unbeschalteter Glasfaserkabel, sind keine passiven Netzinfrastrukturen;

17c. „Premium-Dienste" Dienste, insbesondere der Rufnummernbereiche (0)190 und (0)900, bei denen über die Telekommunikationsdienstleistung hinaus eine weitere Dienstleistung erbracht wird, die gegenüber dem Anrufer gemeinsam mit der Telekommunikationsdienstleistung abgerechnet wird und die nicht einer anderen Nummernart zuzurechnen ist;

18. „Rufnummer" eine Nummer, durch deren Wahl im öffentlich zugänglichen Telefondienst eine Verbindung zu einem bestimmten Ziel aufgebaut werden kann;

18a. „Rufnummernbereich" eine für eine Nummernart bereitgestellte Teilmenge des Nummernraums für das öffentliche Telefonnetz;

18b. „Schnittstelle" ein Netzabschlusspunkt, das heißt, der physische Anschlusspunkt, über den der Benutzer Zugang zu öffentlichen Telekommunikationsnetzen erhält;

19. „Standortdaten" Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben;

19a. „Teilabschnitt" eine Teilkomponente des Teilnehmeranschlusses, die den Netzabschlusspunkt am Standort des Teilnehmers mit einem Konzentrationspunkt oder einem festgelegten zwischengeschalteten Zugangspunkt des öffentlichen Festnetzes verbindet;

20. „Teilnehmer" jede natürliche oder juristische Person, die mit einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat;

21. „Teilnehmeranschluss" die physische Verbindung, mit dem der Netzabschlusspunkt in den Räumlichkeiten des Teilnehmers mit den Hauptverteilerknoten oder mit einer gleichwertigen Einrichtung in festen öffentlichen Telefonnetzen verbunden wird;

22. „Telekommunikation" der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen;

23. „Telekommunikationsanlagen" technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können;

24. „Telekommunikationsdienste" in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen;

24a. „Telekommunikationsendeinrichtung“ eine direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über elektrisch leitenden Draht, über optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Telekommunikationsendeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet;

25. „telekommunikationsgestützte Dienste” Dienste, die keinen räumlich und zeitlich trennbaren Leistungsfluss auslösen, sondern bei denen die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird;

26. „Telekommunikationslinien“ unter- oder oberirdisch geführte Telekommunikationskabelanlagen, einschließlich ihrer zugehörigen Schalt- und Verzweigungseinrichtungen, Masten und Unterstützungen, Kabelschächte und Kabelkanalrohre, sowie weitere technische Einrichtungen, die für das Erbringen von öffentlich zugänglichen Telekommunikationsdiensten erforderlich sind;

27. „Telekommunikationsnetz” die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen, leitungs- und paketvermittelten Netzen, einschließlich des Internets, und mobilen terrestrischen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information;

27a. „Überbau“ die nachträgliche Dopplung von Telekommunikationsinfrastrukturen durch parallele Errichtung, soweit damit dasselbe Versorgungsgebiet erschlossen werden soll;

28. „Übertragungsweg” Telekommunikationsanlagen in Form von Kabel- oder Funkverbindungen mit ihren übertragungstechnischen Einrichtungen als Punkt-zu-Punkt- oder Punkt-zu-Mehrpunktverbindungen mit einem bestimmten Informationsdurchsatzvermögen (Bandbreite oder Bitrate) einschließlich ihrer Abschlusseinrichtungen;

28a. „umfangreiche Renovierungen“ Tief- oder Hochbauarbeiten am Standort des Endnutzers, die strukturelle Veränderungen an den gesamten gebäudeinternen passiven Netzinfrastrukturen oder einem wesentlichen Teil davon umfassen;

29. „Unternehmen” das Unternehmen selbst oder mit ihm im Sinne des § 36 Abs. 2 und § 37 Abs. 1 und 2 des Gesetzes gegen Wettbewerbsbeschränkungen verbundene Unternehmen;

30. „Verkehrsdaten” Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden;

30a. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Datensicherheit, die zum Verlust, zur unrechtmäßigen Löschung, Veränderung, Speicherung, Weitergabe oder sonstigen unrechtmäßigen Verwendung personenbezogener Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste verarbeitet werden sowie der unrechtmäßige Zugang zu diesen;

30b. „vollständig entbündelter Zugang zum Teilnehmeranschluss“ die Bereitstellung des Zugangs zum Teilnehmeranschluss oder zum Teilabschnitt in der Weise, dass die Nutzung der gesamten Kapazität der Netzinfrastruktur ermöglicht wird;

30c. „Warteschleife“ jede vom Nutzer eines Telekommunikationsdienstes eingesetzte Vorrichtung oder Geschäftspraxis, über die Anrufe entgegengenommen oder aufrechterhalten werden, ohne dass das Anliegen des Anrufers bearbeitet wird. Dies umfasst die Zeitspanne ab Rufaufbau vom Anschluss des Anrufers bis zu dem Zeitpunkt, an dem mit der Bearbeitung des Anliegens des Anrufers begonnen wird, gleichgültig ob dies über einen automatisierten Dialog oder durch eine persönliche Bearbeitung erfolgt. Ein automatisierter Dialog beginnt, sobald automatisiert Informationen abgefragt werden, die für die Bearbeitung des Anliegens erforderlich sind. Eine persönliche Bearbeitung des Anliegens beginnt, sobald eine natürliche Person den Anruf entgegennimmt und bearbeitet. Hierzu zählt auch die Abfrage von Informationen, die für die Bearbeitung des Anliegens erforderlich sind. Als Warteschleife ist ferner die Zeitspanne anzusehen, die anlässlich einer Weiterleitung zwischen Beendigung der vorhergehenden Bearbeitung des Anliegens und der weiteren Bearbeitung vergeht, ohne dass der Anruf technisch unterbrochen wird. Keine Warteschleife sind automatische Bandansagen, wenn die Dienstleistung für den Anrufer vor Herstellung der Verbindung erkennbar ausschließlich in einer Bandansage besteht;

31. „wirksamer Wettbewerb” die Abwesenheit von beträchtlicher Marktmacht im Sinne des § 11 Absatz 1 Satz 3 und 4;

32. „Zugang“ die Bereitstellung von Einrichtungen oder Diensten für ein anderes Unternehmen unter bestimmten Bedingungen zum Zwecke der Erbringung von Telekommunikationsdiensten, auch bei deren Verwendung zur Erbringung von Diensten der Informationsgesellschaft oder Rundfunkinhaltediensten. Dies umfasst unter anderem Folgendes:

    a) Zugang zu Netzkomponenten, einschließlich nicht aktiver Netzkomponenten, und zugehörigen Einrichtungen, wozu auch der feste oder nicht feste Anschluss von Geräten gehören kann. Dies beinhaltet insbesondere den Zugang zum Teilnehmeranschluss sowie zu Einrichtungen und Diensten, die erforderlich sind, um Dienste über den Teilnehmeranschluss zu erbringen, einschließlich des Zugangs zur Anschaltung und Ermöglichung des Anbieterwechsels des Teilnehmers und zu hierfür notwendigen Informationen und Daten und zur Entstörung;

b) Zugang zu physischen Infrastrukturen wie Gebäuden, Leitungsrohren und Masten;

c) Zugang zu einschlägigen Softwaresystemen, einschließlich Systemen für die Betriebsunterstützung;

d) Zugang zu informationstechnischen Systemen oder Datenbanken für Vorbestellung, Bereitstellung, Auftragserteilung, Anforderung von Wartungs- und Instandsetzungsarbeiten sowie Abrechnung;

e) Zugang zur Nummernumsetzung oder zu Systemen, die eine gleichwertige Funktion bieten;

f) Zugang zu Fest- und Mobilfunknetzen, insbesondere, um Roaming zu ermöglichen;

g) Zugang zu Zugangsberechtigungssystemen für Digitalfernsehdienste und

h) Zugang zu Diensten für virtuelle Netze;

33. „Zugangsberechtigungssysteme" technische Verfahren oder Vorrichtungen, welche die erlaubte Nutzung geschützter Rundfunkprogramme von einem Abonnement oder einer individuellen Erlaubnis abhängig machen;

33a. „Zugangspunkt zu passiven gebäudeinternen Netzkomponenten" ein physischer Punkt innerhalb oder außerhalb des Gebäudes, der für Eigentümer und Betreiber öffentlicher Telekommunikationsnetze zugänglich ist und den Anschluss an die hochgeschwindigkeitsfähigen gebäudeinternen passiven Netzinfrastrukturen ermöglicht;

33b. „zugehörige Dienste" diejenigen mit einem Telekommunikationsnetz oder einem Telekommunikationsdienst verbundenen Dienste, welche die Bereitstellung von Diensten über dieses Netz oder diesen Dienst ermöglichen, unterstützen oder dazu in der Lage sind. *2*Darunter fallen unter anderem Systeme zur Nummernumsetzung oder Systeme, die eine gleichwertige Funktion bieten, Zugangsberechtigungssysteme und elektronische Programmführer sowie andere Dienste wie Dienste im Zusammenhang mit Identität, Standort und Präsenz des Nutzers;

33c. „zugehörige Einrichtungen" diejenigen mit einem Telekommunikationsnetz oder einem Telekommunikationsdienst verbundenen zugehörigen Dienste, physischen Infrastrukturen und sonstigen Einrichtungen und Komponenten, welche die Bereitstellung von Diensten über dieses Netz oder diesen Dienst ermöglichen, unterstützen oder dazu in der Lage sind. Darunter fallen unter anderem Gebäude, Gebäudezugänge, Verkabelungen in Gebäuden, Antennen, Türme und andere Trägerstrukturen, Leitungsrohre, Leerrohre, Masten, Einstiegsschächte und Verteilerkästen;

34. „Zusammenschaltung" derjenige Zugang, der die physische und logische Verbindung öffentlicher Telekommunikationsnetze herstellt, um Nutzern eines Unternehmens die Kom-

munikation mit Nutzern desselben oder eines anderen Unternehmens oder die Inanspruchnahme von Diensten eines anderen Unternehmens zu ermöglichen; Dienste können von den beteiligten Parteien erbracht werden oder von anderen Parteien, die Zugang zum Netz haben. Zusammenschaltung ist ein Sonderfall des Zugangs und wird zwischen Betreibern öffentlicher Telekommunikationsnetze hergestellt.

§ 4 Internationale Berichtspflichten

Die Betreiber von öffentlichen Telekommunikationsnetzen und die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten müssen der Bundesnetzagentur auf Verlangen die Informationen zur Verfügung stellen, die diese benötigt, um Berichtspflichten gegenüber der Kommission und anderen internationalen Gremien erfüllen zu können.

§ 5 Medien der Veröffentlichung

Veröffentlichungen und Bekanntmachungen, zu denen die Bundesnetzagentur durch dieses Gesetz verpflichtet ist, erfolgen in deren Amtsblatt und auf deren Internetseite, soweit keine abweichende Regelung getroffen ist. *2*Im Amtsblatt der Bundesnetzagentur sind auch technische Richtlinien bekannt zu machen.

§ 6 Meldepflicht

(1) Wer gewerblich öffentliche Telekommunikationsnetze betreibt oder gewerblich öffentlich zugängliche Telekommunikationsdienste erbringt, muss die Aufnahme, Änderung und Beendigung seiner Tätigkeit sowie Änderungen seiner Firma bei der Bundesnetzagentur unverzüglich melden. Die Erklärung bedarf der Schriftform.

(2) Die Meldung muss die Angaben enthalten, die für die Identifizierung des Betreibers oder Anbieters nach Absatz 1 erforderlich sind, insbesondere die Handelsregisternummer, die Anschrift, die Kurzbeschreibung des Netzes oder Dienstes sowie den voraussichtlichen Termin für die Aufnahme der Tätigkeit. Die Meldung hat nach einem von der Bundesnetzagentur vorgeschriebenen und veröffentlichten Formular zu erfolgen.

(3) Auf Antrag bestätigt die Bundesnetzagentur innerhalb von einer Woche die Vollständigkeit der Meldung nach Absatz 2 und bescheinigt, dass dem Unternehmen die durch dieses Gesetz oder auf Grund dieses Gesetzes eingeräumten Rechte zustehen.

(4) Die Bundesnetzagentur veröffentlicht regelmäßig ein Verzeichnis der gemeldeten Unternehmen.

(5) Steht die Einstellung der Geschäftstätigkeit eindeutig fest und ist die Beendigung der Tätigkeit der Bundesnetzagentur nicht innerhalb eines Zeitraums von sechs Monaten schriftlich

gemeldet worden, kann die Bundesnetzagentur die Beendigung der Tätigkeit von Amts wegen feststellen.

§ 43 Vorteilsabschöpfung durch die Bundesnetzagentur

(1) Hat ein Unternehmen gegen eine Verfügung der Bundesnetzagentur nach § 42 Abs. 4 oder vorsätzlich oder fahrlässig gegen eine Vorschrift dieses Gesetzes verstoßen und dadurch einen wirtschaftlichen Vorteil erlangt, soll die Bundesnetzagentur die Abschöpfung des wirtschaftlichen Vorteils anordnen und dem Unternehmen die Zahlung eines entsprechenden Geldbetrags auferlegen.

(2) Absatz 1 gilt nicht, sofern der wirtschaftliche Vorteil durch Schadensersatzleistungen oder durch die Verhängung oder die Anordnung der Einziehung von Taterträgen ausgeglichen ist. Soweit das Unternehmen Leistungen nach Satz 1 erst nach der Vorteilsabschöpfung erbringt, ist der abgeführte Geldbetrag in Höhe der nachgewiesenen Zahlungen an das Unternehmen zurückzuerstatten.

(3) Wäre die Durchführung einer Vorteilsabschöpfung eine unbillige Härte, soll die Anordnung auf einen angemessenen Geldbetrag beschränkt werden oder ganz unterbleiben. Sie soll auch unterbleiben, wenn der wirtschaftliche Vorteil gering ist.

(4) Die Höhe des wirtschaftlichen Vorteils kann geschätzt werden. Der abzuführende Geldbetrag ist zahlenmäßig zu bestimmen.

(5) Die Vorteilsabschöpfung kann nur innerhalb einer Frist von fünf Jahren seit Beendigung der Zuwiderhandlung und längstens für einen Zeitraum von fünf Jahren angeordnet werden.

Teil 3 Kundenschutz

§ 43a Verträge

(1) Anbieter von öffentlich zugänglichen Telekommunikationsdiensten müssen dem Verbraucher und auf Verlangen anderen Endnutzern im Vertrag in klarer, umfassender und leicht zugänglicher Form folgende Informationen zur Verfügung stellen:

1. den Namen und die ladungsfähige Anschrift; ist der Anbieter eine juristische Person auch die Rechtsform, den Sitz und das zuständige Registergericht,

2. die Art und die wichtigsten technischen Leistungsdaten der angebotenen Telekommunikationsdienste, insbesondere diejenigen gemäß Absatz 2 und Absatz 3 Satz 1,

3. die voraussichtliche Dauer bis zur Bereitstellung eines Anschlusses,

4. die angebotenen Wartungs- und Kundendienste sowie die Möglichkeiten zur Kontaktaufnahme mit diesen Diensten,

5. Einzelheiten zu den Preisen der angebotenen Telekommunikationsdienste,

6. die Fundstelle eines allgemein zugänglichen, vollständigen und gültigen Preisverzeichnisses des Anbieters von öffentlich zugänglichen Telekommunikationsdiensten,

7. die Vertragslaufzeit, einschließlich des Mindestumfangs und der Mindestdauer der Nutzung, die gegebenenfalls erforderlich sind, um Angebote im Rahmen von Werbemaßnahmen nutzen zu können,

8. die Voraussetzungen für die Verlängerung und Beendigung des Bezuges einzelner Dienste und des gesamten Vertragsverhältnisses, einschließlich der Voraussetzungen für einen Anbieterwechsel nach § 46, die Entgelte für die Übertragung von Nummern und anderen Teilnehmerkennungen sowie die bei Beendigung des Vertragsverhältnisses fälligen Entgelte einschließlich einer Kostenanlastung für Endeinrichtungen,

9. etwaige Entschädigungs- und Erstattungsregelungen für den Fall, dass der Anbieter die wichtigsten technischen Leistungsdaten der zu erbringenden Dienste nicht eingehalten hat,

10. die erforderlichen Schritte zur Einleitung eines außergerichtlichen Streitbeilegungsverfahrens nach § 47a,

11. den Anspruch des Teilnehmers auf Aufnahme seiner Daten in ein öffentliches Teilnehmerverzeichnis nach § 45m,

12. die Arten von Maßnahmen, mit denen das Unternehmen auf Sicherheits- oder Integritätsverletzungen oder auf Bedrohungen und Schwachstellen reagieren kann,

13. den Anspruch auf Sperrung bestimmter Rufnummernbereiche nach § 45d Absatz 2 Satz 1 und

14. den Anspruch auf Sperrung der Inanspruchnahme und Abrechnung von neben der Verbindung erbrachten Leistungen über den Mobilfunkanschluss nach § 45d Absatz 3.

Anbieter öffentlicher Telekommunikationsnetze sind dazu verpflichtet, Anbietern öffentlich zugänglicher Telekommunikationsdienste die für die Sicherstellung der in Satz 1 genannten Informationspflichten benötigten Informationen zur Verfügung zu stellen, wenn ausschließlich die Anbieter von öffentlichen Telekommunikationsnetzen darüber verfügen.

(2) Zu den Informationen nach Absatz 1 Nummer 2 gehören

1. Informationen darüber, ob der Zugang zu Notdiensten mit Angaben zum Anruferstandort besteht oder nicht, und über alle Beschränkungen von Notdiensten,

2. Informationen über alle Einschränkungen im Hinblick auf den Zugang zu und die Nutzung von Diensten und Anwendungen,

3. das angebotene Mindestniveau der Dienstqualität und gegebenenfalls anderer nach § 41a festgelegter Parameter für die Dienstqualität,

4. Informationen über alle vom Unternehmen zur Messung und Kontrolle des Datenverkehrs eingerichteten Verfahren, um eine Kapazitätsauslastung oder Überlastung einer Netzverbindung zu vermeiden, und Informationen über die möglichen Auswirkungen dieser Verfahren auf die Dienstqualität und

5. alle vom Anbieter auferlegten Beschränkungen für die Nutzung der von ihm zur Verfügung gestellten Endeinrichtungen.

(3) Die Einzelheiten darüber, welche Angaben in der Regel mindestens nach Absatz 2 erforderlich sind, kann die Bundesnetzagentur nach Beteiligung der betroffenen Verbände und der Unternehmen durch Verfügung im Amtsblatt festlegen. Hierzu kann die Bundesnetzagentur die Anbieter öffentlich zugänglicher Telekommunikationsdienste oder die Anbieter öffentlicher Telekommunikationsnetze verpflichten, Erhebungen zum tatsächlichen Mindestniveau der Dienstqualität anzustellen, eigene Messungen anstellen oder Hilfsmittel entwickeln, die es dem Teilnehmer ermöglichen, eigenständige Messungen anzustellen. Die Bundesnetzagentur veröffentlicht jährlich einen Bericht über ihre Erhebungen und Erkenntnisse, in dem insbesondere dargestellt wird,

1. inwiefern die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten die Informationen zur Verfügung stellen, die nach Absatz 2 und nach Artikel 4 Absatz 1 der Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union (ABl. L 310 vom 26.11.2015, S. 1) erforderlich sind,

2. inwiefern erhebliche, kontinuierliche oder regelmäßig wiederkehrende Abweichungen zwischen der nach Satz 2 gemessenen Dienstqualität und den nach Artikel 4 Absatz 1 Unterabsatz 1 Buchstabe d der Verordnung (EU) 2015/2120 im Vertrag enthaltenen Angaben festgestellt wurden und

3. inwiefern Anforderungen und Maßnahmen nach Artikel 5 Absatz 1 Unterabsatz 1 Satz 2 der Verordnung (EU) 2015/2120 notwendig und wirksam sind.

F erner kann die Bundesnetzagentur das Format der Mitteilung über Vertragsänderungen und die anzugebende Information über das Widerrufsrecht festlegen, soweit nicht bereits vergleichbare Regelungen bestehen.

§ 43b Vertragslaufzeit

Die anfängliche Mindestlaufzeit eines Vertrages zwischen einem Verbraucher und einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten darf 24 Monate nicht überschreiten. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sind verpflichtet, einem Teilnehmer zu ermöglichen, einen Vertrag mit einer Höchstlaufzeit von zwölf Monaten abzuschließen.

§ 44 Anspruch auf Schadensersatz und Unterlassung

(1) Ein Unternehmen, das gegen dieses Gesetz, eine auf Grund dieses Gesetzes erlassene Rechtsverordnung, eine auf Grund dieses Gesetzes in einer Zuteilung auferlegte Verpflichtung oder eine Verfügung der Bundesnetzagentur verstößt, ist dem Betroffenen zur Beseitigung und bei Wiederholungsgefahr zur Unterlassung verpflichtet. Der Anspruch besteht bereits dann, wenn eine Zuwiderhandlung droht. Betroffen ist, wer als Endverbraucher oder Wettbewerber durch den Verstoß beeinträchtigt ist. Fällt dem Unternehmen Vorsatz oder Fahrlässigkeit zur Last, ist es einem Endverbraucher oder einem Wettbewerber auch zum Ersatz des Schadens verpflichtet, der ihm aus dem Verstoß entstanden ist. Geldschulden nach Satz 4 hat das Unternehmen ab Eintritt des Schadens zu verzinsen. Die §§ 288 und 289 Satz 1 des Bürgerlichen Gesetzbuchs finden entsprechende Anwendung.

(2) Wer in anderer Weise als durch Verwendung oder Empfehlung von Allgemeinen Geschäftsbedingungen gegen Vorschriften dieses Gesetzes oder Vorschriften einer auf Grund dieses Gesetzes erlassenen Rechtsverordnung verstößt, die dem Schutz der Verbraucher dienen, kann im Interesse des Verbraucherschutzes von den in § 3 des Unterlassungsklagengesetzes genannten Stellen in Anspruch genommen werden. Werden die Zuwiderhandlungen in einem geschäftlichen Betrieb von einem Angestellten oder einem Beauftragten begangen, so ist der Unterlassungsanspruch auch gegen den Inhaber des Betriebes begründet. Im Übrigen bleibt das Unterlassungsklagengesetz unberührt.

§ 44a Haftung

Soweit eine Verpflichtung des Anbieters von öffentlich zugänglichen Telekommunikationsdiensten zum Ersatz eines Vermögensschadens gegenüber einem Endnutzer besteht und nicht auf Vorsatz beruht, ist die Haftung auf höchstens 12 500 Euro je Endnutzer begrenzt. Entsteht die Schadenersatzpflicht durch eine einheitliche Handlung oder ein einheitliches Schaden verursachendes Ereignis gegenüber mehreren Endnutzern und beruht dies nicht auf Vorsatz, so ist die Schadenersatzpflicht unbeschadet der Begrenzung in Satz 1 in der Summe auf höchstens 10 Millionen Euro begrenzt. Übersteigen die Entschädigungen, die mehreren Geschädigten auf Grund desselben Ereignisses zu leisten sind, die Höchstgrenze, so wird der Schadenersatz in dem Verhältnis gekürzt, in dem die Summe aller Schadenersatzansprüche zur Höchstgrenze steht. Die Haftungsbegrenzung nach den Sätzen 1 bis 3 gilt nicht für Ansprüche auf Ersatz des Schadens, der durch den

Verzug der Zahlung von Schadenersatz entsteht. Abweichend von den Sätzen 1 bis 3 kann die Höhe der Haftung gegenüber Endnutzern, die keine Verbraucher sind, durch einzelvertragliche Vereinbarung geregelt werden.

§ 45 Berücksichtigung der Interessen behinderter Endnutzer

(1) Die Interessen behinderter Endnutzer sind von den Anbietern öffentlich zugänglicher Telekommunikationsdienste bei der Planung und Erbringung der Dienste zu berücksichtigen. Es ist ein Zugang zu ermöglichen, der dem Zugang gleichwertig ist, über den die Mehrheit der Endnutzer verfügt. Der Zugang zu den Telekommunikationsdiensten muss behinderten Endnutzern jederzeit zur Verfügung stehen. Gleiches gilt für die Auswahl an Unternehmen und Diensten.

(2) Nach Anhörung der betroffenen Verbände und der Unternehmen kann die Bundesnetzagentur den allgemeinen Bedarf nach Absatz 1 feststellen, der sich aus den Bedürfnissen der behinderten Endnutzer ergibt. Zur Sicherstellung des Dienstes sowie der Dienstemerkmale ist die Bundesnetzagentur befugt, den Unternehmen Verpflichtungen aufzuerlegen. Die Bundesnetzagentur kann von solchen Verpflichtungen absehen, wenn eine Anhörung der betroffenen Kreise ergibt, dass diese Dienstemerkmale oder vergleichbare Dienste als weithin verfügbar erachtet werden.

(3) Die Anbieter öffentlich zugänglicher Telefondienste stellen jederzeit verfügbare Vermittlungsdienste für gehörlose und hörgeschädigte Endnutzer zu einem erschwinglichen Preis unter Berücksichtigung ihrer besonderen Bedürfnisse bereit. Die Bundesnetzagentur ermittelt den Bedarf für diese Vermittlungsdienste unter Beteiligung der betroffenen Verbände und der Unternehmen. Soweit Unternehmen keinen bedarfsgerechten Vermittlungsdienst bereitstellen, beauftragt die Bundesnetzagentur einen Leistungserbringer mit der Bereitstellung eines Vermittlungsdienstes zu einem erschwinglichen Preis. Die mit dieser Bereitstellung nicht durch die vom Nutzer zu zahlenden Entgelte gedeckten Kosten tragen die Unternehmen, die keinen bedarfsgerechten Vermittlungsdienst bereitstellen. Der jeweils von einem Unternehmen zu tragende Anteil an diesen Kosten bemisst sich nach dem Verhältnis des Anteils der vom jeweiligen Unternehmen erbrachten abgehenden Verbindungen zum Gesamtvolumen der von allen zahlungspflichtigen Unternehmen erbrachten abgehenden Verbindungen und wird von der Bundesnetzagentur festgesetzt. Die Zahlungspflicht entfällt für Unternehmen, die weniger als 0,5 Prozent des Gesamtvolumens der abgehenden Verbindungen erbracht haben; der auf diese Unternehmen entfallende Teil der Kosten wird von den übrigen Unternehmen nach Maßgabe des Satzes 5 getragen. Die Bundesnetzagentur legt die Einzelheiten des Verfahrens durch Verfügung fest.

§ 45a Nutzung von Grundstücken

(1) Ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten, der einen Zugang zu einem öffentlichen Telekommunikationsnetz anbietet, darf den Vertrag mit dem Teilnehmer ohne Einhaltung einer Frist kündigen, wenn der Teilnehmer auf Verlangen des Anbieters nicht innerhalb eines Monats den Antrag des dinglich Berechtigten auf Abschluss eines Vertrags zu einer Nutzung des Grundstücks nach der Anlage zu diesem Gesetz (Nutzungsvertrag) vorlegt oder der dinglich Berechtigte den Nutzungsvertrag kündigt.

(2) Sind der Antrag fristgerecht vorgelegt und ein früherer Nutzungsvertrag nicht gekündigt worden, darf der Teilnehmer den Vertrag ohne Einhaltung einer Frist kündigen, wenn der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten den Antrag des Eigentümers auf Abschluss eines Nutzungsvertrags diesem gegenüber nicht innerhalb eines Monats durch Übersendung des von ihm unterschriebenen Vertrags annimmt.

(3) Sofern der Eigentümer keinen weiteren Nutzungsvertrag geschlossen hat und eine Mitbenutzung vorhandener Leitungen und Vorrichtungen des Anbieters von öffentlich zugänglichen Telekommunikationsdiensten durch einen weiteren Anbieter nicht die vertragsgemäße Erfüllung der Verpflichtungen des Anbieters gefährdet oder beeinträchtigt, hat der aus dem Nutzungsvertrag berechtigte Anbieter einem anderen Anbieter auf Verlangen die Mitbenutzung der auf dem Grundstück und in den darauf befindlichen Gebäuden verlegten Leitungen und angebrachten Vorrichtungen des Anbieters zu gewähren. Der Anbieter darf für die Mitbenutzung ein Entgelt erheben, das sich an den Kosten der effizienten Leistungsbereitstellung orientiert.

(4) Geht das Eigentum des Grundstücks auf einen Dritten über, gilt § 566 des Bürgerlichen Gesetzbuchs entsprechend.

§ 45b Entstörungsdienst

Der Teilnehmer kann von einem Anbieter eines öffentlich zugänglichen Telefondienstes verlangen, dass dieser einer Störung unverzüglich, auch nachts und an Sonn- und Feiertagen, nachgeht, wenn der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten über beträchtliche Marktmacht verfügt.

§ 45c Normgerechte technische Dienstleistung

(1) Der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten ist gegenüber dem Teilnehmer verpflichtet, die nach Artikel 17 Absatz 4 der Richtlinie 2002/21/EG verbindlich geltenden Normen für und die technischen Anforderungen an die Bereitstellung von Telekommunikation für Endnutzer einzuhalten.

(2) Die Bundesnetzagentur soll auf die verbindlichen Normen und technischen Anforderungen in Veröffentlichungen hinweisen.

§ 45d Netzzugang

(1) Der Zugang zu öffentlichen Telekommunikationsnetzen an festen Standorten ist an einer mit dem Teilnehmer zu vereinbarenden, geeigneten Stelle zu installieren. Dieser Zugang ist ein passiver Netzabschlusspunkt; das öffentliche Telekommunikationsnetz endet am passiven Netzabschlusspunkt.

(2) Der Teilnehmer kann von dem Anbieter öffentlich zugänglicher Telefondienste und von dem Anbieter des Anschlusses an das öffentliche Telekommunikationsnetz verlangen, dass die Nutzung seines Netzzugangs für bestimmte Rufnummernbereiche im Sinne von § 3 Nummer 18a unentgeltlich netzseitig gesperrt wird, soweit dies technisch möglich ist. Die Freischaltung der gesperrten Rufnummernbereiche kann kostenpflichtig sein.

(3) Der Teilnehmer kann von dem Anbieter öffentlich zugänglicher Mobilfunkdienste und von dem Anbieter des Anschlusses an das öffentliche Mobilfunknetz verlangen, dass die Identifizierung seines Mobilfunkanschlusses zur Inanspruchnahme und Abrechnung einer neben der Verbindung erbrachten Leistung unentgeltlich netzseitig gesperrt wird.

(4) Die Bundesnetzagentur legt nach Anhörung der betroffenen Unternehmen, Fachkreise und Verbraucherverbände Verfahren fest, die die Anbieter öffentlich zugänglicher Mobilfunkdienste und die Anbieter des Anschlusses an das öffentliche Mobilfunknetz anwenden müssen, um die Identifizierung eines Mobilfunkanschlusses zur Inanspruchnahme und Abrechnung einer neben der Verbindung erbrachten Leistung zu nutzen. Diese Verfahren sollen den Teilnehmer wirksam davor schützen, dass eine neben der Verbindung erbrachte Leistung gegen seinen Willen in Anspruch genommen und abgerechnet wird. Die Bundesnetzagentur veröffentlicht die Verfahren und überprüft sie in regelmäßigen Abständen auf ihre Wirksamkeit.

§ 45e Anspruch auf Einzelverbindungsnachweis

(1) Der Teilnehmer kann von dem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten jederzeit mit Wirkung für die Zukunft eine nach Einzelverbindungen aufgeschlüsselte Rechnung (Einzelverbindungsnachweis) verlangen, die zumindest die Angaben enthält, die für eine Nachprüfung der Teilbeträge der Rechnung erforderlich sind. Dies gilt nicht, soweit technische Hindernisse der Erteilung von Einzelverbindungsnachweisen entgegenstehen oder wegen der Art der Leistung eine Rechnung grundsätzlich nicht erteilt wird. Die Rechtsvorschriften zum Schutz personenbezogener Daten bleiben unberührt.

(2) Die Einzelheiten darüber, welche Angaben in der Regel mindestens für einen Einzelverbindungsnachweis nach Absatz 1 Satz 1 erforderlich und in welcher Form diese Angaben jeweils mindestens zu erteilen sind, kann die Bundesnetzagentur durch Verfügung im Amtsblatt festlegen. Der Teilnehmer kann einen auf diese Festlegungen beschränkten Einzelverbindungsnachweis verlangen, für den kein Entgelt erhoben werden darf.

§ 45f Vorausbezahlte Leistung

Der Teilnehmer muss die Möglichkeit haben, auf Vorauszahlungsbasis Zugang zum öffentlichen Telekommunikationsnetz zu erhalten oder öffentlich zugängliche Telefondienste in Anspruch nehmen zu können. Die Einzelheiten kann die Bundesnetzagentur durch Verfügung im Amtsblatt festlegen. Für den Fall, dass eine entsprechende Leistung nicht angeboten wird, schreibt die Bundesnetzagentur die Leistung aus. Für das Verfahren gilt § 81 Abs. 2, 4 und 5 entsprechend.

§ 45g Verbindungspreisberechnung

(1) Bei der Abrechnung ist der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten verpflichtet,

1. die Dauer und den Zeitpunkt zeitabhängig tarifierter Verbindungen von öffentlich zugänglichen Telekommunikationsdiensten unter regelmäßiger Abgleichung mit einem amtlichen Zeitnormal zu ermitteln,

2. die für die Tarifierung relevanten Entfernungszonen zu ermitteln,

3. die übertragene Datenmenge bei volumenabhängig tarifierten Verbindungen von öffentlich zugänglichen Telekommunikationsdiensten nach einem nach Absatz 3 vorgegebenen Verfahren zu ermitteln und

4. die Systeme, Verfahren und technischen Einrichtungen, mit denen auf der Grundlage der ermittelten Verbindungsdaten die Entgeltforderungen berechnet werden, einer regelmäßigen Kontrolle auf Abrechnungsgenauigkeit und Übereinstimmung mit den vertraglich vereinbarten Entgelten zu unterziehen.

(2) Die Voraussetzungen nach Absatz 1 Nr. 1, 2 und 3 sowie Abrechnungsgenauigkeit und Entgeltrichtigkeit der Datenverarbeitungseinrichtungen nach Absatz 1 Nr. 4 sind durch ein Qualitätssicherungssystem sicherzustellen oder einmal jährlich durch öffentlich bestellte und vereidigte Sachverständige oder vergleichbare Stellen überprüfen zu lassen. Zum Nachweis der Einhaltung dieser Bestimmung ist der Bundesnetzagentur die Prüfbescheinigung einer akkreditierten Zertifizierungsstelle für Qualitätssicherungssysteme oder das Prüfergebnis eines öffentlich bestellten und vereidigten Sachverständigen vorzulegen.

(3) Die Bundesnetzagentur legt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik Anforderungen an die Systeme und Verfahren zur Ermittlung des Entgelts volumenabhängig tarifierter Verbindungen nach Absatz 1 Nr. 2, 3 und 4 nach Anhörung der betroffenen Unternehmen, Fachkreise und Verbraucherverbände durch Verfügung im Amtsblatt fest.

§ 45h Rechnungsinhalt, Teilzahlungen

(1) Soweit ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten dem Teilnehmer eine Rechnung stellt, die auch Entgelte für Leistungen Dritter ausweist, muss die Rechnung des Anbieters in einer hervorgehobenen und deutlich gestalteten Form Folgendes enthalten:

1. die konkrete Bezeichnung der in Rechnung gestellten Leistungen,
2. die Namen und ladungsfähigen Anschriften beteiligter Anbieter von Netzdienstleistungen,
3. einen Hinweis auf den Informationsanspruch des Teilnehmers nach § 45p,
4. die kostenfreien Kundendiensttelefonnummern der Anbieter von Netzdienstleistungen und des rechnungsstellenden Anbieters, unter denen der Teilnehmer die Informationen nach § 45p erlangen kann,
5. die Gesamthöhe der auf jeden Anbieter entfallenden Entgelte.

§ 45e bleibt unberührt. Zahlt der Teilnehmer den Gesamtbetrag der Rechnung an den rechnungsstellenden Anbieter, so befreit ihn diese Zahlung von der Zahlungsverpflichtung auch gegenüber den anderen auf der Rechnung aufgeführten Anbietern.

(2) Hat der Teilnehmer vor oder bei der Zahlung nichts Anderes bestimmt, so sind Teilzahlungen des Teilnehmers an den rechnungsstellenden Anbieter auf die in der Rechnung ausgewiesenen Forderungen nach ihrem Anteil an der Gesamtforderung der Rechnung zu verrechnen.

(3) Das rechnungsstellende Unternehmen muss den Rechnungsempfänger in der Rechnung darauf hinweisen, dass dieser berechtigt ist, begründete Einwendungen gegen einzelne in der Rechnung gestellte Forderungen zu erheben.

(4) (weggefallen)

(5) Die Einzelheiten darüber, welche Angaben nach Absatz 1 Satz 1 Nummer 3 auf der Rechnung mindestens für einen transparenten und nachvollziehbaren Hinweis auf den Informationsanspruch des Teilnehmers nach § 45p erforderlich sind, kann die Bundesnetzagentur durch Verfügung im Amtsblatt festlegen.

§ 45i Beanstandungen

(1) Der Teilnehmer kann eine ihm von dem Anbieter von Telekommunikationsdiensten erteilte Abrechnung innerhalb einer Frist von mindestens acht Wochen nach Zugang der Rechnung beanstanden. Im Falle der Beanstandung hat der Anbieter das in Rechnung gestellte Verbindungsaufkommen unter Wahrung der datenschutzrechtlichen Belange etwaiger weiterer Nutzer des Anschlusses als Entgeltnachweis nach den einzelnen Verbindungsdaten aufzuschlüsseln und eine technische Prüfung durchzuführen, es sei denn, die Beanstandung ist nachweislich nicht auf einen technischen Mangel zurückzuführen. Der Teilnehmer kann innerhalb der Beanstandungsfrist verlangen, dass ihm der Entgeltnachweis und die Ergebnisse der technischen Prüfung vorgelegt werden. Erfolgt eine nach Satz 3 verlangte Vorlage nicht binnen acht Wochen nach einer Beanstandung, erlöschen bis dahin entstandene Ansprüche aus Verzug; die mit der Abrechnung geltend gemachte Forderung wird mit der nach Satz 3 verlangten Vorlage fällig. Die Bundesnetzagentur veröffentlicht, welche Verfahren zur Durchführung der technischen Prüfung geeignet sind.

(2) Soweit aus technischen Gründen keine Verkehrsdaten gespeichert oder für den Fall, dass keine Beanstandungen erhoben wurden, gespeicherte Daten nach Verstreichen der in Absatz 1 Satz 1 geregelten oder mit dem Anbieter vereinbarten Frist oder auf Grund rechtlicher Verpflichtungen gelöscht worden sind, trifft den Anbieter weder eine Nachweispflicht für die erbrachten Verbindungsleistungen noch die Auskunftspflicht nach Absatz 1 für die Einzelverbindungen. Satz 1 gilt entsprechend, soweit der Teilnehmer nach einem deutlich erkennbaren Hinweis auf die Folgen nach Satz 1 verlangt hat, dass Verkehrsdaten gelöscht oder nicht gespeichert werden.

(3) Dem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten obliegt der Nachweis, dass er den Telekommunikationsdienst oder den Zugang zum Telekommunikationsnetz bis zu dem Übergabepunkt, an dem dem Teilnehmer der Netzzugang bereitgestellt wird, technisch fehlerfrei erbracht hat. Ergibt die technische Prüfung nach Absatz 1 Mängel, die sich auf die Berechnung des beanstandeten Entgelts zu Lasten des Teilnehmers ausgewirkt haben können, oder wird die technische Prüfung später als zwei Monate nach der Beanstandung durch den Teilnehmer abgeschlossen, wird widerleglich vermutet, dass das in Rechnung gestellte Verbindungsaufkommen des jeweiligen Anbieters von öffentlich zugänglichen Telekommunikationsdiensten unrichtig ermittelt ist.

(4) Soweit der Teilnehmer nachweist, dass ihm die Inanspruchnahme von Leistungen des Anbieters nicht zugerechnet werden kann, hat der Anbieter keinen Anspruch auf Entgelt gegen den Teilnehmer. Der Anspruch entfällt auch, soweit Tatsachen die Annahme rechtfertigen, dass Dritte durch unbefugte Veränderungen an öffentlichen Telekommunikationsnetzen das in Rechnung gestellte Verbindungsentgelt beeinflusst haben.

§ 45j Entgeltpflicht bei unrichtiger Ermittlung des Verbindungsaufkommens

(1) Kann im Falle des § 45i Abs. 3 Satz 2 das tatsächliche Verbindungsaufkommen nicht festgestellt werden, hat der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten gegen den Teilnehmer Anspruch auf den Betrag, den der Teilnehmer in den vorangegangenen sechs Abrechnungszeiträumen durchschnittlich als Entgelt für einen entsprechenden Zeitraum zu entrichten hatte. Dies gilt nicht, wenn der Teilnehmer nachweist, dass er in dem Abrechnungszeitraum den Netzzugang nicht oder in geringerem Umfang als nach der Durchschnittsberechnung genutzt hat. Die Sätze 1 und 2 gelten entsprechend, wenn nach den Umständen erhebliche Zweifel bleiben, ob dem Teilnehmer die Inanspruchnahme von Leistungen des Anbieters zugerechnet werden kann.

(2) Soweit in der Geschäftsbeziehung zwischen Anbieter und Teilnehmer weniger als sechs Abrechnungszeiträume unbeanstandet geblieben sind, wird die Durchschnittsberechnung nach Absatz 1 auf die verbleibenden Abrechnungszeiträume gestützt. Bestand in den entsprechenden Abrechnungszeiträumen eines Vorjahres bei vergleichbaren Umständen durchschnittlich eine niedrigere Entgeltforderung, tritt dieser Betrag an die Stelle des nach Satz 1 berechneten Durchschnittsbetrags.

(3) Fordert der Anbieter ein Entgelt auf der Grundlage einer Durchschnittsberechnung, so gilt das von dem Teilnehmer auf die beanstandete Forderung zu viel gezahlte Entgelt spätestens zwei Monate nach der Beanstandung als fällig.

§ 45k Sperre

(1) Der Anbieter öffentlich zugänglicher Telefondienste darf zu erbringende Leistungen an einen Teilnehmer unbeschadet anderer gesetzlicher Vorschriften nur nach Maßgabe der Absätze 2 bis 5 und nach § 45o Satz 3 ganz oder teilweise verweigern (Sperre). § 108 Abs. 1 bleibt unberührt.

(2) Wegen Zahlungsverzugs darf der Anbieter eine Sperre durchführen, wenn der Teilnehmer nach Abzug etwaiger Anzahlungen mit Zahlungsverpflichtungen von mindestens 75 Euro in Verzug ist und der Anbieter die Sperre mindestens zwei Wochen zuvor schriftlich angedroht und dabei auf die Möglichkeit des Teilnehmers, Rechtsschutz vor den Gerichten zu suchen, hingewiesen hat. Bei der Berechnung der Höhe des Betrags nach Satz 1 bleiben nicht titulierte Forderungen, die der Teilnehmer form- und fristgerecht und schlüssig begründet beanstandet hat, außer Betracht. Ebenso bleiben nicht titulierte bestrittene Forderungen Dritter im Sinne des § 45h Absatz 1 Satz 1 außer Betracht. Dies gilt auch dann, wenn diese Forderungen abgetreten worden sind. Die Bestimmungen der Sätze 2 bis 4 gelten nicht, wenn der Anbieter den Teilnehmer zuvor zur vorläufigen Zahlung eines Durchschnittsbetrags nach § 45j aufgefordert und der Teilnehmer diesen nicht binnen zwei Wochen gezahlt hat.

(3) Der Anbieter darf seine Leistung einstellen, sobald die Kündigung des Vertragsverhältnisses wirksam wird.

(4) Der Anbieter darf eine Sperre durchführen, wenn wegen einer im Vergleich zu den vorangegangenen sechs Abrechnungszeiträumen besonderen Steigerung des Verbindungsaufkommens auch die Höhe der Entgeltforderung des Anbieters in besonderem Maße ansteigt und Tatsachen die Annahme rechtfertigen, dass der Teilnehmer diese Entgeltforderung beanstanden wird.

(5) Die Sperre ist, soweit technisch möglich und dem Anlass nach sinnvoll, auf bestimmte Leistungen zu beschränken. Sie darf nur aufrechterhalten werden, solange der Grund für die Sperre fortbesteht. Eine auch ankommende Telekommunikationsverbindung erfassende Vollsperrung des Netzzugangs darf frühestens eine Woche nach Sperrung abgehender Telekommunikationsverbindungen erfolgen.

§ 45l Dauerschuldverhältnisse bei Kurzwahldiensten

(1) Der Teilnehmer kann von dem Anbieter einer Dienstleistung, die zusätzlich zu einem öffentlich zugänglichen Telekommunikationsdienst erbracht wird, einen kostenlosen Hinweis verlangen, sobald dessen Entgeltansprüche aus Dauerschuldverhältnissen für Kurzwahldienste im jeweiligen Kalendermonat eine Summe von 20 Euro überschreiten. Der Anbieter ist nur zur unverzüglichen Absendung des Hinweises verpflichtet. Für Kalendermonate, vor deren Beginn der Teilnehmer einen Hinweis nach Satz 1 verlangt hat und in denen der Hinweis unterblieben ist, kann der Anbieter nach Satz 1 den 20 Euro überschreitenden Betrag nicht verlangen.

(2) Der Teilnehmer kann ein Dauerschuldverhältnis für Kurzwahldienste zum Ende eines Abrechnungszeitraumes mit einer Frist von einer Woche gegenüber dem Anbieter kündigen. Der Abrechnungszeitraum darf die Dauer eines Monats nicht überschreiten. Abweichend von Satz 1 kann der Teilnehmer ein Dauerschuldverhältnis für Kurzwahldienste, das ereignisbasiert ist, jederzeit und ohne Einhaltung einer Frist gegenüber dem Anbieter kündigen.

(3) Vor dem Abschluss von Dauerschuldverhältnissen für Kurzwahldienste, bei denen für die Entgeltansprüche des Anbieters jeweils der Eingang elektronischer Nachrichten beim Teilnehmer maßgeblich ist, hat der Anbieter dem Teilnehmer eine deutliche Information über die wesentlichen Vertragsbestandteile anzubieten. Zu den wesentlichen Vertragsbestandteilen gehören insbesondere der zu zahlende Preis einschließlich Steuern und Abgaben je eingehender Kurzwahlsendung, der Abrechnungszeitraum, die Höchstzahl der eingehenden Kurzwahlsendungen im Abrechnungszeitraum, sofern diese Angaben nach Art der Leistung möglich sind, das jederzeitige Kündigungsrecht sowie die notwendigen praktischen Schritte für eine Kündigung. Ein Dauerschuldverhältnis für Kurzwahldienste entsteht

nicht, wenn der Teilnehmer den Erhalt der Informationen nach Satz 1 nicht bestätigt; dennoch geleistete Zahlungen des Teilnehmers an den Anbieter sind zurückzuzahlen.

§ 45m Aufnahme in öffentliche Teilnehmerverzeichnisse

(1) Der Teilnehmer kann von seinem Anbieter eines öffentlichen Telefondienstes jederzeit verlangen, mit seiner Rufnummer, seinem Namen, seinem Vornamen und seiner Anschrift in ein allgemein zugängliches, nicht notwendig anbietereigenes Teilnehmerverzeichnis unentgeltlich eingetragen zu werden oder seinen Eintrag wieder löschen zu lassen. Einen unrichtigen Eintrag hat der Anbieter zu berichtigen. Der Teilnehmer kann weiterhin jederzeit verlangen, dass Mitbenutzer seines Zugangs mit Namen und Vornamen eingetragen werden, soweit Rechtsvorschriften zum Schutz personenbezogener Daten nicht entgegenstehen; für diesen Eintrag darf ein Entgelt erhoben werden.

(2) Die Ansprüche nach Absatz 1 stehen auch Wiederverkäufern von Sprachkommunikationsdienstleistungen für deren Teilnehmer zu.

(3) Die Absätze 1 und 2 gelten entsprechend für die Aufnahme in Verzeichnisse für Auskunftsdienste.

§ 45n Transparenz, Veröffentlichung von Informationen und zusätzliche Dienstemerkmale zur Kostenkontrolle

(1) Das Bundesministerium für Wirtschaft und Energie wird ermächtigt, im Einvernehmen mit dem Bundesministerium des Innern, dem Bundesministerium der Justiz und für Verbraucherschutz sowie dem Bundesministerium für Verkehr und digitale Infrastruktur durch Rechtsverordnung mit Zustimmung des Bundestages Rahmenvorschriften zur Förderung der Transparenz sowie zur Veröffentlichung von Informationen und zusätzlichen Dienstemerkmalen zur Kostenkontrolle auf dem Telekommunikationsmarkt zu erlassen.

(2) In der Rechtsverordnung nach Absatz 1 können Anbieter von öffentlichen Telekommunikationsnetzen und Anbieter öffentlich zugänglicher Telekommunikationsdienste verpflichtet werden, dem Verbraucher und auf Verlangen anderen Endnutzern transparente, vergleichbare, ausreichende und aktuelle Informationen bereitzustellen:

1. über geltende Preise und Tarife,
2. über den Vertragsbeginn, die noch verbleibende Vertragslaufzeit und die bei Vertragskündigung anfallenden Gebühren,
3. über Standardbedingungen für den Zugang zu den von ihnen für Endnutzer und Verbraucher bereitgestellten Diensten und deren Nutzung,

4. über die Dienstqualität einschließlich eines Angebotes zur Überprüfbarkeit der Datenübertragungsrate und

5. über die Maßnahmen, die zur Gewährleistung der Gleichwertigkeit beim Zugang für behinderte Endnutzer getroffen worden sind.

(3) Im Rahmen des Absatzes 2 Nummer 3 können Anbieter von öffentlichen Telekommunikationsnetzen und Anbieter öffentlich zugänglicher Telekommunikationsdienste verpflichtet werden, dem Verbraucher und auf Verlangen anderen Endnutzern Folgendes bereitzustellen:

1. den Namen und die ladungsfähige Anschrift, bei juristischen Personen auch die Rechtsform, den Sitz und das zuständige Registergericht,

2. den Umfang der angebotenen Dienste einschließlich der Bedingungen für Datenvolumenbeschränkungen,

3. Einzelheiten zu den Preisen der angebotenen Dienste, Dienstemerkmalen und Wartungsdiensten einschließlich etwaiger besonderer Preise für bestimmte Endnutzergruppen sowie Kosten für Endeinrichtungen,

4. Einzelheiten zu ihren Entschädigungs- und Erstattungsregelungen und deren Handhabung,

5. ihre Allgemeinen Geschäftsbedingungen und die von ihnen angebotenen Mindestvertragslaufzeiten, die Voraussetzungen für einen Anbieterwechsel nach § 46, Kündigungsbedingungen sowie Verfahren und direkte Entgelte im Zusammenhang mit der Übertragung von Rufnummern oder anderen Kennungen,

6. allgemeine und anbieterbezogene Informationen über die Verfahren zur Streitbeilegung und

7. Informationen über grundlegende Rechte der Endnutzer von Telekommunikationsdiensten, insbesondere

   a) zu Einzelverbindungsnachweisen,

   b) zu beschränkten und für den Endnutzer kostenlosen Sperren abgehender Verbindungen oder von Kurzwahl-Datendiensten oder, soweit technisch möglich, anderer Arten ähnlicher Anwendungen,

   c) zur Nutzung öffentlicher Telekommunikationsnetze gegen Vorauszahlung,

   d) zur Verteilung der Kosten für einen Netzanschluss auf einen längeren Zeitraum,

   e) zu den Folgen von Zahlungsverzug für mögliche Sperren und

f) zu den Dienstemerkmalen Tonwahl- und Mehrfrequenzwahlverfahren und Anzeige der Rufnummer des Anrufers.

(4) In der Rechtsverordnung nach Absatz 1 können Anbieter von öffentlichen Telekommunikationsnetzen und Anbieter öffentlich zugänglicher Telekommunikationsdienste unter anderem verpflichtet werden,

1. bei Nummern oder Diensten, für die eine besondere Preisgestaltung gilt, den Teilnehmern die dafür geltenden Tarife anzugeben; für einzelne Kategorien von Diensten kann verlangt werden, diese Informationen unmittelbar vor Herstellung der Verbindung bereitzustellen,

2. die Teilnehmer über jede Änderung des Zugangs zu Notdiensten oder der Angaben zum Anruferstandort bei dem Dienst, bei dem sie angemeldet sind, zu informieren,

3. die Teilnehmer über jede Änderung der Einschränkungen im Hinblick auf den Zugang zu und die Nutzung von Diensten und Anwendungen zu informieren,

4. Informationen bereitzustellen über alle vom Betreiber zur Messung und Kontrolle des Datenverkehrs eingerichteten Verfahren, um eine Kapazitätsauslastung oder Überlastung einer Netzverbindung zu vermeiden, und über die möglichen Auswirkungen dieser Verfahren auf die Dienstqualität,

5. nach Artikel 12 der Richtlinie 2002/58/EG die Teilnehmer über ihr Recht auf eine Entscheidung über Aufnahme oder Nichtaufnahme ihrer personenbezogenen Daten in ein Teilnehmerverzeichnis und über die Art der betreffenden Daten zu informieren sowie

6. behinderte Teilnehmer regelmäßig über Einzelheiten der für sie bestimmten Produkte und Dienste zu informieren.

Falls dies als zweckdienlich erachtet wird, können in der Verordnung auch Verfahren zur Selbst- oder Koregulierung vorgesehen werden.

(5) Die Informationen sind in klarer, verständlicher und leicht zugänglicher Form dem Verbraucher und auf Verlangen anderen Endnutzern bereitzustellen. In der Rechtsverordnung nach Absatz 1 können hinsichtlich Ort und Form der Bereitstellung weitere Anforderungen festgelegt werden.

(6) In der Rechtsverordnung nach Absatz 1 können Anbieter öffentlich zugänglicher Telefondienste und Anbieter öffentlicher Telekommunikationsnetze verpflichtet werden,

1. eine Einrichtung anzubieten, mit der der Teilnehmer auf Antrag bei den Anbietern abgehende Verbindungen oder Kurzwahl-Datendienste oder andere Arten ähnlicher Anwendungen oder bestimmte Arten von Nummern kostenlos sperren lassen kann,

2. eine Einrichtung anzubieten, mit der der Teilnehmer bei seinem Anbieter die Identifizierung

eines Mobilfunkanschlusses zur Inanspruchnahme und Abrechnung einer neben der Verbindung erbrachten Leistung unentgeltlich netzseitig sperren lassen kann,

3. Verbrauchern einen Anschluss an das öffentliche Telekommunikationsnetz auf der Grundlage zeitlich gestreckter Zahlungen zu gewähren,

4. eine Einrichtung anzubieten, mit der der Teilnehmer vom Anbieter Informationen über etwaige preisgünstigere alternative Tarife des jeweiligen Unternehmens anfordern kann, oder

5. eine geeignete Einrichtung anzubieten, um die Kosten öffentlich zugänglicher Telekommunikationsdienste zu kontrollieren, einschließlich unentgeltlicher Warnhinweise für die Verbraucher bei anormalem oder übermäßigem Verbraucherverhalten, die sich an Artikel 6a Absatz 1 bis 3 der Verordnung (EG) Nr. 717/2007 des Europäischen Parlaments und des Rates vom 27. Juni 2007 über das Roaming in öffentlichen Mobilfunknetzen in der Gemeinschaft und zur Änderung der Richtlinie 2002/21/EG (ABl. L 171 vom 29.6.2007, S. 32), die zuletzt durch die Verordnung (EG) Nr. 544/2009 (ABl. L 167 vom 29.6.2009, S. 12) geändert worden ist, orientiert.

Eine Verpflichtung zum Angebot der zusätzlichen Dienstemerkmale nach Satz 1 kommt nach Berücksichtigung der Ansichten der Betroffenen nicht in Betracht, wenn bereits in ausreichendem Umfang Zugang zu diesen Dienstemerkmalen besteht.

(7) Das Bundesministerium für Wirtschaft und Energie kann im Einvernehmen mit dem Bundesministerium für Verkehr und digitale Infrastruktur die Ermächtigung nach Absatz 1 durch Rechtsverordnung an die Bundesnetzagentur übertragen. Eine Rechtsverordnung der Bundesnetzagentur bedarf des Einvernehmens mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium des Innern, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Verkehr und digitale Infrastruktur und dem Bundestag.

(8) Die Bundesnetzagentur kann in ihrem Amtsblatt oder auf ihrer Internetseite jegliche Information veröffentlichen, die für Endnutzer Bedeutung haben kann. Sonstige Rechtsvorschriften, namentlich zum Schutz personenbezogener Daten und zum Presserecht, bleiben unberührt. Die Bundesnetzagentur kann zur Bereitstellung von vergleichbaren Informationen nach Absatz 1 interaktive Führer oder ähnliche Techniken selbst oder über Dritte bereitstellen, wenn diese auf dem Markt nicht kostenlos oder zu einem angemessenen Preis zur Verfügung stehen. Zur Bereitstellung nach Satz 3 ist die Nutzung der von Anbietern von Telekommunikationsnetzen und von Anbietern öffentlich zugänglicher Telekommunikationsdienste veröffentlichten Informationen für die Bundesnetzagentur oder für Dritte kostenlos.

§ 45o Rufnummernmissbrauch

Wer Rufnummern in seinem Telekommunikationsnetz einrichtet, hat den Zuteilungsnehmer schriftlich darauf hinzuweisen, dass die Übersendung und Übermittlung von Informationen, Sachen oder sonstige Leistungen unter bestimmten Umständen gesetzlich verboten ist. Hat er gesicherte Kenntnis davon, dass eine in seinem Telekommunikationsnetz eingerichtete Rufnummer unter Verstoß gegen Satz 1 genutzt wird, ist er verpflichtet, unverzüglich Maßnahmen zu ergreifen, die geeignet sind, eine Wiederholung zu verhindern. Bei wiederholten oder schwerwiegenden Verstößen gegen gesetzliche Verbote ist der Anbieter nach erfolgloser Abmahnung unter kurzer Fristsetzung verpflichtet, die Rufnummer zu sperren.

§ 45p Auskunftsanspruch über zusätzliche Leistungen

(1) Stellt der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten dem Teilnehmer eine Rechnung, die auch Entgelte für Leistungen Dritter ausweist, so muss er dem Teilnehmer auf Verlangen unverzüglich kostenfrei folgende Informationen zur Verfügung stellen:

1. die Namen und ladungsfähigen Anschriften der Dritten,

2. bei Diensteanbietern mit Sitz im Ausland zusätzlich die ladungsfähige Anschrift eines allgemeinen Zustellungsbevollmächtigten im Inland.

Die gleiche Verpflichtung trifft auch den beteiligten Anbieter von Netzdienstleistungen.

(2) Der verantwortliche Anbieter einer neben der Verbindung erbrachten Leistung muss auf Verlangen des Teilnehmers diesen über den Grund und Gegenstand des Entgeltanspruchs, der nicht ausschließlich Gegenleistung einer Verbindungsleistung ist, insbesondere über die Art der erbrachten Leistung, unterrichten.

§ 46 Anbieterwechsel und Umzug

(1) Die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten und die Betreiber öffentlicher Telekommunikationsnetze müssen bei einem Anbieterwechsel sicherstellen, dass die Leistung des abgebenden Unternehmens gegenüber dem Teilnehmer nicht unterbrochen wird, bevor die vertraglichen und technischen Voraussetzungen für einen Anbieterwechsel vorliegen, es sei denn, der Teilnehmer verlangt dieses. Bei einem Anbieterwechsel darf der Dienst des Teilnehmers nicht länger als einen Kalendertag unterbrochen werden. Schlägt der Wechsel innerhalb dieser Frist fehl, gilt Satz 1 entsprechend.

(2) Das abgebende Unternehmen hat ab Beendigung der vertraglich vereinbarten Leistung bis zum Ende der Leistungspflicht nach Absatz 1 Satz 1 gegenüber dem Teilnehmer einen Anspruch auf Entgeltzahlung. Die Höhe des Entgelts richtet sich nach den ursprünglich

vereinbarten Vertragsbedingungen mit der Maßgabe, dass sich die vereinbarten Anschlussentgelte um 50 Prozent reduzieren, es sei denn, das abgebende Unternehmen weist nach, dass der Teilnehmer das Scheitern des Anbieterwechsels zu vertreten hat. Das abgebende Unternehmen hat im Fall des Absatzes 1 Satz 1 gegenüber dem Teilnehmer eine taggenaue Abrechnung vorzunehmen. Der Anspruch des aufnehmenden Unternehmens auf Entgeltzahlung gegenüber dem Teilnehmer entsteht nicht vor erfolgreichem Abschluss des Anbieterwechsels.

(3) Um den Anbieterwechsel nach Absatz 1 zu gewährleisten, müssen Betreiber öffentlicher Telekommunikationsnetze in ihren Netzen insbesondere sicherstellen, dass Teilnehmer ihre Rufnummer unabhängig von dem Unternehmen, das den Telefondienst erbringt, wie folgt beibehalten können:

1. im Fall geografisch gebundener Rufnummern an einem bestimmten Standort und

2. im Fall nicht geografisch gebundener Rufnummern an jedem Standort.

Die Regelung in Satz 1 gilt nur innerhalb der Nummernräume oder Nummerteilräume, die für einen Telefondienst festgelegt wurden. Insbesondere ist die Übertragung von Rufnummern für Telefondienste an festen Standorten zu solchen ohne festen Standort und umgekehrt unzulässig.

(4) Um den Anbieterwechsel nach Absatz 1 zu gewährleisten, müssen Anbieter von öffentlich zugänglichen Telekommunikationsdiensten insbesondere sicherstellen, dass ihre Endnutzer ihnen zugeteilte Rufnummern bei einem Wechsel des Anbieters von öffentlich zugänglichen Telekommunikationsdiensten entsprechend Absatz 3 beibehalten können. Die technische Aktivierung der Rufnummer hat in jedem Fall innerhalb eines Kalendertages zu erfolgen. Für die Anbieter öffentlich zugänglicher Mobilfunkdienste gilt Satz 1 mit der Maßgabe, dass der Endnutzer jederzeit die Übertragung der zugeteilten Rufnummer verlangen kann. Der bestehende Vertrag zwischen Endnutzer und abgebendem Anbieter öffentlich zugänglicher Mobilfunkdienste bleibt davon unberührt; hierauf hat der aufnehmende Anbieter den Endnutzer vor Vertragsschluss in Textform hinzuweisen. Der abgebende Anbieter ist in diesem Fall verpflichtet, den Endnutzer zuvor über alle anfallenden Kosten zu informieren. Auf Verlangen hat der abgebende Anbieter dem Endnutzer eine neue Rufnummer zuzuteilen.

(5) Dem Teilnehmer können nur die Kosten in Rechnung gestellt werden, die einmalig beim Wechsel entstehen. Das Gleiche gilt für die Kosten, die ein Netzbetreiber einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten in Rechnung stellt. Etwaige Entgelte unterliegen einer nachträglichen Regulierung nach Maßgabe des § 38 Absatz 2 bis 4.

(6) Betreiber öffentlicher Telekommunikationsnetze haben in ihren Netzen sicherzustellen, dass alle Anrufe in den europäischen Telefonnummernraum ausgeführt werden.

(7) Die Erklärung des Teilnehmers zur Einrichtung oder Änderung der Betreibervorauswahl oder die von ihm erteilte Vollmacht zur Abgabe dieser Erklärung bedarf der Textform.

(8) Der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten, der mit einem Verbraucher einen Vertrag über öffentlich zugängliche Telekommunikationsdienste geschlossen hat, ist verpflichtet, wenn der Verbraucher seinen Wohnsitz wechselt, die vertraglich geschuldete Leistung an dem neuen Wohnsitz des Verbrauchers ohne Änderung der vereinbarten Vertragslaufzeit und der sonstigen Vertragsinhalte zu erbringen, soweit diese dort angeboten wird. Der Anbieter kann ein angemessenes Entgelt für den durch den Umzug entstandenen Aufwand verlangen, das jedoch nicht höher sein darf als das für die Schaltung eines Neuanschlusses vorgesehene Entgelt. Wird die Leistung am neuen Wohnsitz nicht angeboten, ist der Verbraucher zur Kündigung des Vertrages unter Einhaltung einer Kündigungsfrist von drei Monaten zum Ende eines Kalendermonats berechtigt. In jedem Fall ist der Anbieter des öffentlich zugänglichen Telekommunikationsdienstes verpflichtet, den Anbieter des öffentlichen Telekommunikationsnetzes über den Auszug des Verbrauchers unverzüglich zu informieren, wenn der Anbieter des öffentlich zugänglichen Telekommunikationsdienstes Kenntnis vom Umzug des Verbrauchers erlangt hat.

(9) Die Bundesnetzagentur kann die Einzelheiten des Verfahrens für den Anbieterwechsel und die Informationsverpflichtung nach Absatz 8 Satz 4 festlegen. Dabei ist insbesondere Folgendes zu berücksichtigen:

1. das Vertragsrecht,
2. die technische Entwicklung,
3. die Notwendigkeit, dem Teilnehmer die Kontinuität der Dienstleistung zu gewährleisten, und
4. erforderlichenfalls Maßnahmen, die sicherstellen, dass Teilnehmer während des gesamten Übertragungsverfahrens geschützt sind und nicht gegen ihren Willen auf einen anderen Anbieter umgestellt werden.

Für Teilnehmer, die keine Verbraucher sind und mit denen der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten eine Individualvereinbarung getroffen hat, kann die Bundesnetzagentur von Absatz 1 und 2 abweichende Regelungen treffen. Die Befugnisse nach Teil 2 dieses Gesetzes und nach § 77a Absatz 1 und Absatz 2 bleiben unberührt.

§ 47 Bereitstellen von Teilnehmerdaten

(1) Jedes Unternehmen, das öffentlich zugängliche Telekommunikationsdienste erbringt und Rufnummern an Endnutzer vergibt, ist verpflichtet, unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen, jedem Unternehmen auf Antrag Teilnehmerdaten

nach Absatz 2 Satz 4 zum Zwecke der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten, Diensten zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers nach § 95 Absatz 2 Satz 1 und Teilnehmerverzeichnissen zur Verfügung zu stellen. Die Überlassung der Daten hat unverzüglich und in nichtdiskriminierender Weise zu erfolgen.

(2) Teilnehmerdaten sind die nach Maßgabe des § 104 in Teilnehmerverzeichnissen veröffentlichten Daten. Hierzu gehören neben der Nummer sowohl die zu veröffentlichenden Daten selbst wie Name, Anschrift und zusätzliche Angaben wie Beruf, Branche, Art des Anschlusses und Mitbenutzer, soweit sie dem Unternehmen vorliegen. Dazu gehören auch alle nach dem jeweiligen Stand der Technik unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen in kundengerechter Form aufbereiteten Informationen, Verknüpfungen, Zuordnungen und Klassifizierungen, die zur Veröffentlichung dieser Daten in öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen nach Satz 1 notwendig sind. Die Daten müssen vollständig und inhaltlich sowie technisch so aufbereitet sein, dass sie nach dem jeweiligen Stand der Technik ohne Schwierigkeiten in ein kundenfreundlich gestaltetes Teilnehmerverzeichnis oder eine entsprechende Auskunftsdienstedatenbank aufgenommen werden können.

(3) Ergeben sich Streitigkeiten zwischen Unternehmen über die Rechte und Verpflichtungen aus den Absätzen 1 und 2, gilt § 133 entsprechend.

(4) Für die Überlassung der Teilnehmerdaten kann ein Entgelt erhoben werden; dieses unterliegt in der Regel einer nachträglichen Regulierung nach Maßgabe des § 38 Abs. 2 bis 4. Ein solches Entgelt soll nur dann einer Genehmigungspflicht nach § 31 unterworfen werden, wenn das Unternehmen auf dem Markt für Endnutzerleistungen über eine beträchtliche Marktmacht verfügt.

§ 47a Schlichtung

(1) Kommt es zwischen dem Teilnehmer und einem Betreiber von öffentlichen Telekommunikationsnetzen oder einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten zum Streit darüber, ob der Betreiber oder Anbieter dem Teilnehmer gegenüber eine Verpflichtung erfüllt hat, die sich auf die Bedingungen oder die Ausführung der Verträge über die Bereitstellung dieser Netze oder Dienste bezieht und mit folgenden Regelungen zusammenhängt:

1. §§ 43a, 43b, 45 bis 46 oder den auf Grund dieser Regelungen erlassenen Rechtsverordnungen und § 84 oder

2. der Verordnung (EU) Nr. 531/2012 des Europäischen Parlaments und des Rates vom 13. Juni 2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union (ABl. L 172 vom

30.6.2012, S. 10), die zuletzt durch die Verordnung (EU) 2015/2120 (ABl. L 310 vom 26.11.2015, S. 1) geändert worden ist,

3. Artikel 4 Absatz 1, 2 und 4 der Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union, kann der Teilnehmer bei der Verbraucherschlichtungsstelle der Bundesnetzagentur durch einen Antrag ein Schlichtungsverfahren einleiten.

(2) Das Schlichtungsverfahren endet, wenn

1. der Schlichtungsantrag zurückgenommen wird,

2. der Teilnehmer und der Anbieter sich geeinigt und dies der Bundesnetzagentur mitgeteilt haben,

3. der Teilnehmer und der Anbieter übereinstimmend erklären, dass sich der Streit erledigt hat,

4. die Verbraucherschlichtungsstelle der Bundesnetzagentur dem Teilnehmer und dem Anbieter schriftlich mitteilt, dass eine Einigung im Schlichtungsverfahren nicht erreicht werden konnte, oder

5. die Verbraucherschlichtungsstelle der Bundesnetzagentur feststellt, dass Belange nach Absatz 1 nicht mehr berührt sind.

(3) Die Bundesnetzagentur regelt die weiteren Einzelheiten über das Schlichtungsverfahren in einer Schlichtungsordnung, die sie veröffentlicht. Die Verbraucherschlichtungsstelle der Bundesnetzagentur muss die Anforderungen nach dem Verbraucherstreitbeilegungsgesetz vom 19. Februar 2016 (BGBl. | S. 254) erfüllen. Das Bundesministerium für Wirtschaft und Energie übermittelt der Zentralen Anlaufstelle für Verbraucherschlichtung die Mitteilungen nach § 32 Absatz 3 und 5 des Verbraucherstreitbeilegungsgesetzes.

§ 47b Abweichende Vereinbarungen

Von den Vorschriften dieses Teils oder der auf Grund dieses Teils erlassenen Rechtsverordnungen darf, soweit nicht ein Anderes bestimmt ist, nicht zum Nachteil des Teilnehmers abgewichen werden.

Abschnitt 2 Nummerierung

§ 66 Nummerierung

(1) Die Bundesnetzagentur nimmt die Aufgaben der Nummerierung wahr. Ihr obliegt insbesondere die Strukturierung und Ausgestaltung des Nummernraumes mit dem Ziel, den Anforderungen von Endnutzern, Betreibern von Telekommunikationsnetzen und Anbietern von Telekommunikationsdiensten zu genügen. Die Bundesnetzagentur teilt ferner Nummern an Betreiber von Telekommunikationsnetzen, Anbieter von Telekommunikationsdiensten und Endnutzer zu. Ausgenommen ist die Verwaltung von Domänennamen oberster und nachgeordneter Stufen.

(2) Die Bundesnetzagentur kann zur Umsetzung internationaler Verpflichtungen oder Empfehlungen sowie zur Sicherstellung der ausreichenden Verfügbarkeit von Nummern Änderungen der Struktur und Ausgestaltung des Nummernraumes und des nationalen Nummernplanes vornehmen. Dabei sind die Belange der Betroffenen, insbesondere die den Betreibern, Anbietern von Telekommunikationsdiensten und Nutzern entstehenden Umstellungskosten, angemessen zu berücksichtigen. Beabsichtigte Änderungen sind rechtzeitig vor ihrem Wirksamwerden bekannt zu geben. Die von diesen Änderungen betroffenen Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten sind verpflichtet, die zur Umsetzung erforderlichen Maßnahmen zu treffen.

(3) Die Bundesnetzagentur kann zur Durchsetzung der Verpflichtungen nach Absatz 2 Anordnungen erlassen. Zur Durchsetzung der Anordnungen können nach Maßgabe des Verwaltungsvollstreckungsgesetzes Zwangsgelder bis zu 500 000 Euro festgesetzt werden.

(4) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die Maßstäbe und Leitlinien für die Strukturierung, Ausgestaltung und Verwaltung der Nummernräume sowie für den Erwerb, Umfang und Verlust von Nutzungsrechten an Nummern festzulegen. Dies schließt auch die Umsetzung darauf bezogener internationaler Empfehlungen und Verpflichtungen in nationales Recht ein. Dabei sind insbesondere die effiziente Nummernnutzung, die Belange der Marktbeteiligten einschließlich der Planungssicherheit, die wirtschaftlichen Auswirkungen auf die Marktteilnehmer, die Anforderungen an die Nummernnutzung und die langfristige Bedarfsdeckung sowie die Interessen der Endnutzer zu berücksichtigen. In der Verordnung sind die Befugnisse der Bundesnetzagentur sowie die Rechte und Pflichten der Marktteilnehmer und der Endnutzer im Einzelnen festzulegen. Absatz 1 Satz 4 gilt entsprechend.

(5) Ist im Vergabeverfahren für generische Domänen oberster Stufe für die Zuteilung oder Verwendung einer geografischen Bezeichnung, die mit dem Namen einer Gebietskörperschaft identisch ist, eine Einverständniserklärung oder Unbedenklichkeitsbescheinigung durch eine deutsche Regierungs- oder Verwaltungsstelle erforderlich, obliegt die Entscheidung

über die Erteilung des Einverständnisses oder die Ausstellung einer Unbedenklichkeitsbescheinigung der nach dem jeweiligen Landesrecht zuständigen Stelle. Weisen mehrere Gebietskörperschaften identische Namen auf, liegt die Entscheidungsbefugnis bei der Gebietskörperschaft, die nach der Verkehrsauffassung die größte Bedeutung hat.

§ 66a Preisangabe

Wer gegenüber Endnutzern Premium-Dienste, Auskunftsdienste, Massenverkehrsdienste, Service-Dienste, Neuartige Dienste oder Kurzwahldienste anbietet oder dafür wirbt, hat dabei den für die Inanspruchnahme des Dienstes zu zahlenden Preis zeitabhängig je Minute oder zeitunabhängig je Inanspruchnahme einschließlich der Umsatzsteuer und sonstiger Preisbestandteile anzugeben. Bei Angabe des Preises ist der Preis gut lesbar, deutlich sichtbar und in unmittelbarem Zusammenhang mit der Rufnummer anzugeben. Bei Anzeige der Rufnummer darf die Preisangabe nicht zeitlich kürzer als die Rufnummer angezeigt werden. Auf den Abschluss eines Dauerschuldverhältnisses ist hinzuweisen. Soweit für die Inanspruchnahme eines Dienstes nach Satz 1 für Anrufe aus den Mobilfunknetzen Preise gelten, die von den Preisen für Anrufe aus den Festnetzen abweichen, ist der Festnetzpreis mit dem Hinweis auf die Möglichkeit abweichender Preise für Anrufe aus den Mobilfunknetzen anzugeben. Abweichend hiervon ist bei Service-Diensten neben dem Festnetzpreis der Mobilfunkhöchstpreis anzugeben, soweit für die Inanspruchnahme des Dienstes für Anrufe aus den Mobilfunknetzen Preise gelten, die von den Preisen für Anrufe aus den Festnetzen abweichen. Bei Telefax-Diensten ist zusätzlich die Zahl der zu übermittelnden Seiten anzugeben. Bei Datendiensten ist zusätzlich, soweit möglich, der Umfang der zu übermittelnden Daten anzugeben, es sei denn, die Menge der zu übermittelnden Daten hat keine Auswirkung auf die Höhe des Preises für den Endnutzer.

§ 66b Preisansage

(1) Für sprachgestützte Premium-Dienste und für sprachgestützte Betreiberauswahl hat derjenige, der den vom Endnutzer zu zahlenden Preis für die Inanspruchnahme dieses Dienstes festlegt, vor Beginn der Entgeltpflichtigkeit dem Endnutzer den für die Inanspruchnahme dieses Dienstes zu zahlenden Preis zeitabhängig je Minute oder zeitunabhängig je Datenvolumen oder sonstiger Inanspruchnahme einschließlich der Umsatzsteuer und sonstiger Preisbestandteile anzusagen. Die Preisansage ist spätestens drei Sekunden vor Beginn der Entgeltpflichtigkeit unter Hinweis auf den Zeitpunkt des Beginns derselben abzuschließen. Ändert sich dieser Preis während der Inanspruchnahme des Dienstes, so ist vor Beginn des neuen Tarifabschnitts der nach der Änderung zu zahlende Preis entsprechend der Sätze 1 und 2 anzusagen mit der Maßgabe, dass die Ansage auch während der Inanspruchnahme des Dienstes erfolgen kann. Beim Einsatz von Warteschleifen nach § 66g Absatz 1 Nummer 5 stellt weder der Beginn noch das Ende der Warteschleife eine Änderung des Preises im Sinne des Satzes 3 dar, wenn der vom Endnutzer im Sinne des Satzes 1 zu zahlende Preis für den Tarif-

abschnitt nach der Warteschleife unverändert gegenüber dem Preis für den Tarifabschnitt vor der Warteschleife ist. Die Sätze 1 bis 4 gelten auch für sprachgestützte Auskunftsdienste und für Kurzwahl-Sprachdienste ab einem Preis von 2 Euro pro Minute oder pro Inanspruchnahme bei zeitunabhängiger Tarifierung. Die Sätze 1 bis 4 gelten auch für sprachgestützte Neuartige Dienste ab einem Preis von 2 Euro pro Minute oder pro Inanspruchnahme bei zeitunabhängiger Tarifierung, soweit nach Absatz 4 nicht etwas Anderes bestimmt ist.

(2) Bei Inanspruchnahme von Rufnummern für sprachgestützte Massenverkehrs-Dienste hat der Diensteanbieter dem Endnutzer den für die Inanspruchnahme dieser Rufnummer zu zahlenden Preis für Anrufe aus den Festnetzen einschließlich der Umsatzsteuer und sonstiger Preisbestandteile unmittelbar im Anschluss an die Inanspruchnahme des Dienstes anzusagen.

(3) Im Falle der Weitervermittlung durch einen sprachgestützten Auskunftsdienst besteht die Preisansageverpflichtung für das weiterzuvermittelnde Gespräch für den Auskunftsdiensteanbieter. Die Ansage kann während der Inanspruchnahme des sprachgestützten Auskunftsdienstes erfolgen, ist jedoch vor der Weitervermittlung vorzunehmen; Absatz 1 Satz 3 und 4 gilt entsprechend. Diese Ansage umfasst den Preis für Anrufe aus den Festnetzen zeitabhängig je Minute oder zeitunabhängig je Datenvolumen oder sonstiger Inanspruchnahme einschließlich der Umsatzsteuer und sonstiger Preisbestandteile sowie einen Hinweis auf die Möglichkeit abweichender Preise aus dem Mobilfunk.

(4) Bei sprachgestützten Neuartigen Diensten kann die Bundesnetzagentur nach Anhörung der Fachkreise und Verbraucherverbände Anforderungen für eine Preisansage festlegen, die von denen des Absatzes 1 Satz 6 abweichen, sofern technische Entwicklungen, die diesen Nummernbereich betreffen, ein solches Verfahren erforderlich machen. Die Festlegungen sind von der Bundesnetzagentur zu veröffentlichen.

§ 66c Preisanzeige

(1) Für Kurzwahl-Datendienste hat außer im Falle des § 45l derjenige, der den vom Endnutzer zu zahlenden Preis für die Inanspruchnahme dieses Dienstes festlegt, vor Beginn der Entgeltpflichtigkeit den für die Inanspruchnahme dieses Dienstes zu zahlenden Preis einschließlich der Umsatzsteuer und sonstiger Preisbestandteile ab einem Preis von 2 Euro pro Inanspruchnahme deutlich sichtbar und gut lesbar anzuzeigen und sich vom Endnutzer den Erhalt der Information bestätigen zu lassen. Satz 1 gilt auch für nichtsprachgestützte Neuartige Dienste ab einem Preis von 2 Euro pro Inanspruchnahme.

(2) Von den Verpflichtungen nach Absatz 1 kann abgewichen werden, wenn der Dienst im öffentlichen Interesse erbracht wird oder sich der Endkunde vor Inanspruchnahme der Dienstleistung gegenüber dem Verpflichteten nach Absatz 1 durch ein geeignetes Verfahren legitimiert. Die Einzelheiten regelt und veröffentlicht die Bundesnetzagentur.

§ 66d Preishöchstgrenzen

(1) Der Preis für zeitabhängig über Rufnummern für Premium-Dienste abgerechnete Dienstleistungen darf höchstens 3 Euro pro Minute betragen, soweit nach Absatz 4 keine abweichenden Preise erhoben werden können. Dies gilt auch im Falle der Weitervermittlung durch einen Auskunftsdienst. *3*Die Abrechnung darf höchstens im 60-Sekunden-Takt erfolgen.

(2) Der Preis für zeitunabhängig über Rufnummern für Premium-Dienste abgerechnete Dienstleistungen darf höchstens 30 Euro pro Verbindung betragen, soweit nach Absatz 4 keine abweichenden Preise erhoben werden können. Wird der Preis von Dienstleistungen aus zeitabhängigen und zeitunabhängigen Leistungsanteilen gebildet, so müssen diese Preisanteile entweder im Einzelverbindungsnachweis, soweit dieser erteilt wird, getrennt ausgewiesen werden oder Verfahren nach Absatz 4 Satz 3 zur Anwendung kommen. Der Preis nach Satz 2 darf höchstens 30 Euro je Verbindung betragen, soweit nach Absatz 4 keine abweichenden Preise erhoben werden können.

(3) Der Preis für Anrufe bei Service-Diensten darf aus den Festnetzen höchstens 0,14 Euro pro Minute oder 0,20 Euro pro Anruf und aus den Mobilfunknetzen höchstens 0,42 Euro pro Minute oder 0,60 Euro pro Anruf betragen, soweit nach Absatz 4 Satz 4 keine abweichenden Preise erhoben werden können. Die Abrechnung darf höchstens im 60-Sekunden-Takt erfolgen.

(4) Über die Preisgrenzen der Absätze 1 und 2 hinausgehende Preise dürfen nur erhoben werden, wenn sich der Kunde vor Inanspruchnahme der Dienstleistung gegenüber dem Diensteanbieter durch ein geeignetes Verfahren legitimiert. Die Einzelheiten regelt die Bundesnetzagentur. Sie kann durch Verfügung im Amtsblatt Einzelheiten zu zulässigen Verfahren in Bezug auf Tarifierungen nach den Absätzen 1 und 2 und zu den Ausnahmen nach Absatz 2 Satz 2 und 3 festlegen. Darüber hinaus kann die Bundesnetzagentur entsprechend dem Verfahren nach § 67 Abs. 2 von den Absätzen 1 bis 3 abweichende Preishöchstgrenzen festsetzen, wenn die allgemeine Entwicklung der Preise oder des Marktes dies erforderlich macht.

(5) Der Preis für Anrufe in den und aus dem Europäischen Telefonnummerierungsraum (ETNS) muss mit dem jeweils geltenden Höchstpreis für Auslandsanrufe in andere oder aus anderen Mitgliedstaaten vergleichbar sein. Die Einzelheiten regelt die Bundesnetzagentur durch Verfügung im Amtsblatt.

§ 66e Verbindungstrennung

(1) Der Diensteanbieter, bei dem die Rufnummer für Premium-Dienste oder Kurzwahl-Sprachdienste eingerichtet ist, hat jede zeitabhängig abgerechnete Verbindung zu dieser nach 60 Minuten zu trennen. Dies gilt auch, wenn zu einer Rufnummer für Premium-Dienste oder für Kurzwahl-Sprachdienste weitervermittelt wurde.

(2) Von der Verpflichtung nach Absatz 1 kann abgewichen werden, wenn sich der Endnutzer vor der Inanspruchnahme der Dienstleistung gegenüber dem Diensteanbieter durch ein geeignetes Verfahren legitimiert. Die Einzelheiten regelt die Bundesnetzagentur. Sie kann durch Verfügung die Einzelheiten der zulässigen Verfahren zur Verbindungstrennung festlegen.

§ 66f Anwählprogramme (Dialer)

(1) Anwählprogramme, die Verbindungen zu einer Nummer herstellen, bei denen neben der Telekommunikationsdienstleistung Inhalte abgerechnet werden (Dialer), dürfen nur eingesetzt werden, wenn sie vor Inbetriebnahme bei der Bundesnetzagentur registriert wurden, von ihr vorgegebene Mindestvoraussetzungen erfüllen und ihr gegenüber schriftlich versichert wurde, dass eine rechtswidrige Nutzung ausgeschlossen ist. Dialer dürfen nur über Rufnummern aus einem von der Bundesnetzagentur hierzu zur Verfügung gestellten Nummernbereich angeboten werden. *3*Das Betreiben eines nicht registrierten Dialers neben einem registrierten Dialer unter einer Nummer ist unzulässig.

(2) Unter einer Zielrufnummer registriert die Bundesnetzagentur jeweils nur einen Dialer. Änderungen des Dialers führen zu einer neuen Registrierungspflicht. Die Bundesnetzagentur regelt die Einzelheiten des Registrierungsverfahrens und den Inhalt der abzugebenden schriftlichen Versicherung. Sie kann Einzelheiten zur Verwendung des Tarifs für zeitunabhängig abgerechnete Dienstleistungen sowie zur Registrierung von Dialern nach Satz 1 festlegen, soweit diese Verfahren in gleicher Weise geeignet sind, die Belange des Verbraucherschutzes zu gewährleisten, und durch Verfügung veröffentlichen.

(3) Die Bundesnetzagentur kann die Registrierung von Dialern ablehnen, wenn Tatsachen die Annahme rechtfertigen, dass der Antragsteller nicht die erforderliche Zuverlässigkeit besitzt. Dies ist insbesondere der Fall, wenn der Antragsteller schwerwiegend gegen die Vorschriften dieses Gesetzes verstoßen oder wiederholt eine Registrierung durch falsche Angaben erwirkt hat. Im Falle von Satz 1 teilt die Bundesnetzagentur ihre Erkenntnisse den für den Vollzug der Gewerbeordnung zuständigen Stellen mit.

§ 66g Warteschleifen

(1) Warteschleifen dürfen nur eingesetzt werden, wenn eine der folgenden Voraussetzungen erfüllt ist:

1. der Anruf erfolgt zu einer entgeltfreien Rufnummer,

2. der Anruf erfolgt zu einer ortsgebundenen Rufnummer oder einer Rufnummer, die die Bundesnetzagentur den ortsgebundenen Rufnummern nach Absatz 3 gleichgestellt hat,

3. der Anruf erfolgt zu einer Rufnummer für mobile Dienste (015, 016 oder 017),

4. für den Anruf gilt ein Festpreis pro Verbindung oder

5. der Anruf ist für die Dauer der Warteschleife für den Anrufer kostenfrei, soweit es sich nicht um Kosten handelt, die bei Anrufen aus dem Ausland für die Herstellung der Verbindung im Ausland entstehen.

(2) Beim ersten Einsatz einer Warteschleife im Rahmen des Anrufs, die nicht unter Absatz 1 Nummer 1 bis 3 fällt, hat der Angerufene sicherzustellen, dass der Anrufende mit Beginn der Warteschleife über ihre voraussichtliche Dauer und, unbeschadet der §§ 66a bis 66c, darüber informiert wird, ob für den Anruf ein Festpreis gilt oder der Angerufene gemäß Absatz 1 Nummer 5 für die Dauer des Einsatzes dieser Warteschleife für den Anrufer kostenfrei ist. Die Ansage kann mit Beginn der Bearbeitung vorzeitig beendet werden.

(3) Die Bundesnetzagentur stellt auf Antrag des Zuteilungsnehmers Rufnummern den ortsgebundenen Rufnummern nach Absatz 1 Nummer 2 in Bezug auf den Einsatz von Warteschleifen gleich, wenn

1. der Angerufene vom Anrufer weder unmittelbar noch mittelbar über den Anbieter von Telekommunikationsdiensten ein Entgelt für den Anruf zu dieser Nummer erhält und Anrufe zu dieser Nummer in der Regel von den am Markt verfügbaren Pauschaltarifen erfasst sind und

2. die Tarifierung dieser Rufnummer auch im Übrigen keine abweichende Behandlung gegenüber den ortsgebundenen Rufnummern rechtfertigt.

§ 66h Wegfall des Entgeltanspruchs

Der Endnutzer ist zur Zahlung eines Entgelts nicht verpflichtet, wenn und soweit

1. nach Maßgabe des § 66b Abs. 1 nicht vor Beginn der Inanspruchnahme oder nach Maßgabe des § 66b Abs. 2, 3 und 4 nicht während der Inanspruchnahme des Dienstes über den erhobenen Preis informiert oder eine auf Grund des § 45n Absatz 4 Nummer 1 im Rahmen einer Rechtsverordnung erlassene Regelung nicht erfüllt wurde,

2. nach Maßgabe des § 66c nicht vor Beginn der Inanspruchnahme über den erhobenen Preis informiert wurde und keine Bestätigung des Endnutzers erfolgt oder eine auf Grund des § 45n Absatz 4 Nummer 1 im Rahmen einer Rechtsverordnung erlassene Regelung nicht erfüllt wurde,

3. nach Maßgabe des § 66d die Preishöchstgrenzen nicht eingehalten wurden oder gegen die Verfahren zu Tarifierungen nach § 66d Abs. 2 Satz 2 und 3 verstoßen wurde,

4. nach Maßgabe des § 66e die zeitliche Obergrenze nicht eingehalten wurde,

5. Dialer entgegen § 66f Abs. 1 und 2 betrieben wurden,

6. nach Maßgabe des § 66i Abs. 1 Satz 2 R-Gesprächsdienste mit Zahlungen an den Anrufer angeboten werden,

7. nach Maßgabe des § 66i Abs. 2 ein Tag nach Eintrag in die Sperr-Liste ein R-Gespräch zum gesperrten Anschluss erfolgt oder

8. der Angerufene entgegen § 66g Absatz 1 während des Anrufs eine oder mehrere Warteschleifen einsetzt oder die Angaben nach § 66g Absatz 2 nicht, nicht vollständig oder nicht rechtzeitig gemacht werden. *2*In diesen Fällen entfällt die Entgeltzahlungspflicht des Anrufers für den gesamten Anruf.

§ 66i Auskunftsanspruch, Datenbank für (0)900er Rufnummern

(1) Jeder, der ein berechtigtes Interesse daran hat, kann in Textform von der Bundesnetzagentur Auskunft über den Namen und die ladungsfähige Anschrift desjenigen verlangen, der eine Nummer von der Bundesnetzagentur zugeteilt bekommen hat. Die Auskunft soll unverzüglich nach Eingang der Anfrage nach Satz 1 erteilt werden.

(2) Alle zugeteilten (0)900er-Rufnummern werden in einer Datenbank bei der Bundesnetzagentur erfasst. Diese Datenbank ist mit Angabe des Namens und mit der ladungsfähigen Anschrift des Diensteanbieters, bei Diensteanbietern mit Sitz im Ausland zusätzlich der ladungsfähigen Anschrift eines allgemeinen Zustellungsbevollmächtigten im Inland, im Internet zu veröffentlichen. Jedermann kann in Textform von der Bundesnetzagentur Auskunft über die in der Datenbank gespeicherten Daten verlangen.

(3) Jeder, der ein berechtigtes Interesse daran hat, kann von demjenigen, dem von der Bundesnetzagentur Rufnummern für Massenverkehrsdienste, Neuartige Dienste oder Kurzwahldienste zugeteilt sind, unentgeltlich Auskunft über den Namen und die ladungsfähige Anschrift desjenigen verlangen, der über eine dieser Rufnummern Dienstleistungen anbietet, oder die Mitteilung verlangen, an wen die Rufnummer gemäß § 46 übertragen wurde. Bei Kurzwahlnummern, die nicht von der Bundesnetzagentur zugeteilt wurden, besteht der Anspruch gegenüber demjenigen, in dessen Netz die Kurzwahlnummer geschaltet ist. Bei gemäß § 46 übertragenen Rufnummern besteht der Anspruch auf Auskunft über den Namen und die ladungsfähige Anschrift desjenigen, der über eine Rufnummer Dienstleistungen anbietet, gegenüber dem Anbieter, zu dem die Rufnummer übertragen wurde. Die Auskünfte nach den Sätzen 1 bis 3 sollen innerhalb von zehn Werktagen nach Eingang der in Textform gestellten Anfrage erteilt werden. Die Auskunftsverpflichteten haben die Angabe bei ihren Kunden zu erheben und aktuell zu halten.

§ 66j R-Gespräche

(1) Auf Grund von Telefonverbindungen, bei denen dem Angerufenen das Verbindungsentgelt in Rechnung gestellt wird (R-Gespräche), dürfen keine Zahlungen an den Anrufer erfolgen. Das Angebot von R-Gesprächsdiensten mit einer Zahlung an den Anrufer nach Satz 1 ist unzulässig.

(2) Die Bundesnetzagentur führt eine Sperr-Liste mit Rufnummern, die von R-Gesprächsdiensten für eingehende R-Gespräche zu sperren sind. Endkunden können ihren Anbieter von Telekommunikationsdiensten beauftragen, die Aufnahme ihrer Nummern in die Sperr-Liste unentgeltlich zu veranlassen. Eine Löschung von der Liste kann kostenpflichtig sein. Der Anbieter übermittelt den Endkundenwunsch sowie etwaig erforderliche Streichungen wegen Wegfalls der abgeleiteten Zuteilung. Die Bundesnetzagentur stellt die Sperr-Liste Anbietern von R-Gesprächsdiensten zum Abruf bereit.

§ 66k Rufnummernübermittlung

(1) Anbieter von Telekommunikationsdiensten, die Teilnehmern den Aufbau von abgehenden Verbindungen ermöglichen, müssen sicherstellen, dass beim Verbindungsaufbau als Rufnummer des Anrufers eine vollständige national signifikante Rufnummer übermittelt und als solche gekennzeichnet wird. Die Rufnummer muss dem Teilnehmer für den Dienst zugeteilt sein, im Rahmen dessen die Verbindung aufgebaut wird. Deutsche Rufnummern für Auskunftsdienste, Massenverkehrsdienste, Neuartige Dienste oder Premium-Dienste sowie Nummern für Kurzwahl-Sprachdienste dürfen nicht als Rufnummer des Anrufers übermittelt werden. *4*Andere an der Verbindung beteiligte Anbieter dürfen übermittelte Rufnummern nicht verändern.

(2) Teilnehmer dürfen weitere Rufnummern nur aufsetzen und in das öffentliche Telekommunikationsnetz übermitteln, wenn sie ein Nutzungsrecht an der entsprechenden Rufnummer haben. Deutsche Rufnummern für Auskunftsdienste, Massenverkehrsdienste, Neuartige Dienste oder Premium-Dienste sowie Nummern für Kurzwahl-Sprachdienste dürfen von Teilnehmern nicht als zusätzliche Rufnummer aufgesetzt und in das öffentliche Telekommunikationsnetz übermittelt werden.

§ 66l Internationaler entgeltfreier Telefondienst

Anrufe bei (00)800er-Rufnummern müssen für den Anrufer unentgeltlich sein. Die Erhebung eines Entgelts für die Inanspruchnahme eines Endgerätes bleibt unbenommen.

§ 66m Umgehungsverbot

Die Vorschriften der §§ 66a bis 66l oder die auf Grund des § 45n Absatz 4 Nummer 1 im Rahmen einer Rechtsverordnung erlassenen Regelungen sind auch dann anzuwenden, wenn versucht wird, sie durch anderweitige Gestaltungen zu umgehen.

§ 67 Befugnisse der Bundesnetzagentur

(1) Die Bundesnetzagentur kann im Rahmen der Nummernverwaltung Anordnungen und andere geeignete Maßnahmen treffen, um die Einhaltung gesetzlicher Vorschriften und der von ihr erteilten Bedingungen über die Zuteilung von Nummern sicherzustellen. Die Bundesnetzagentur kann die Betreiber von öffentlichen Telekommunikationsnetzen und die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten verpflichten, Auskünfte zu personenbezogenen Daten wie Name und ladungsfähige Anschrift von Nummerninhabern und Nummernnutzern zu erteilen, die für den Vollzug dieses Gesetzes, auf Grund dieses Gesetzes ergangener Verordnungen sowie der erteilten Bedingungen erforderlich sind, soweit die Daten den Unternehmen bekannt sind; die Bundesnetzagentur kann insbesondere Auskünfte zu personenbezogenen Daten verlangen, die erforderlich sind für die einzelfallbezogene Überprüfung von Verpflichtungen, wenn der Bundesnetzagentur eine Beschwerde vorliegt oder sie aus anderen Gründen eine Verletzung von Pflichten annimmt oder sie von sich aus Ermittlungen durchführt. Andere Regelungen bleiben von der Auskunftspflicht nach Satz 2 unberührt. Insbesondere kann die Bundesnetzagentur bei Nichterfüllung von gesetzlichen oder behördlich auferlegten Verpflichtungen die rechtswidrig genutzte Nummer entziehen. Sie soll ferner im Falle der gesicherten Kenntnis von der rechtswidrigen Nutzung einer Rufnummer gegenüber dem Netzbetreiber, in dessen Netz die Nummer geschaltet ist, die Abschaltung der Rufnummer anordnen. Die Bundesnetzagentur kann den Rechnungsersteller bei gesicherter Kenntnis einer rechtswidrigen Nutzung auffordern, für diese Nummer keine Rechnungslegung vorzunehmen. Die Bundesnetzagentur kann in begründeten Ausnahmefällen Kategorien von Dialern verbieten; Einzelheiten des Verbotsverfahrens regelt die Bundesnetzagentur.

(2) Soweit für Premium-Dienste, Massenverkehrsdienste, Service-Dienste oder Neuartige Dienste die Tarifhoheit bei dem Anbieter liegt, der den Teilnehmeranschluss bereitstellt, und deshalb unterschiedliche Entgelte für Anrufe aus den Festnetzen gelten würden, legt die Bundesnetzagentur nach Anhörung der betroffenen Unternehmen, Fachkreise und Verbraucherverbände zum Zwecke der Preisangabe und Preisansage nach den §§ 66a und 66b oder der auf Grund des § 45n Absatz 4 Nummer 1 im Rahmen einer Rechtsverordnung erlassenen Regelungen jeweils bezogen auf bestimmte Nummernbereiche oder Nummernteilbereiche den Preis für Anrufe aus den Festnetzen fest. Für Anrufe aus den Mobilfunknetzen bei Service-Diensten legt die Bundesnetzagentur nach Anhörung der in Satz 1 genannten Stellen fest, ob der Anruf bezogen auf einen bestimmten Nummernteilbereich pro Minute

oder pro Anruf abgerechnet wird; dies gilt nur, soweit die Tarifhoheit bei dem Anbieter liegt, der den Zugang zum Mobilfunknetz bereitstellt. Im Übrigen hat sie sicherzustellen, dass ausreichend frei tarifierbare Nummernbereiche oder Nummernteilbereiche verbleiben. Die festzulegenden Preise haben sich an den im Markt angebotenen Preisen für Anrufe aus den Festnetzen zu orientieren und sind in regelmäßigen Abständen zu überprüfen. Die festzulegenden Preise sind von der Bundesnetzagentur zu veröffentlichen. Die Bestimmungen der §§ 16 bis 26 bleiben unberührt.

(3) Die Rechte der Länder sowie die Befugnisse anderer Behörden bleiben unberührt.

(4) Die Bundesnetzagentur teilt Tatsachen, die den Verdacht einer Straftat oder einer Ordnungswidrigkeit begründen, der Staatsanwaltschaft oder der Verwaltungsbehörde mit.

Teil 7 Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit

Abschnitt 1 Fernmeldegeheimnis

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

§ 89 Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen

Mit einer Funkanlage dürfen nur Nachrichten, die für den Betreiber der Funkanlage, Funkamateure im Sinne des Gesetzes über den Amateurfunk vom 23. Juni 1997 (BGBl. | S. 1494), die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, abgehört oder in vergleichbarer Weise zur Kenntnis genommen werden. Der Inhalt anderer als in Satz 1 genannter Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht zur Geheimhaltung nicht schon nach § 88 besteht, anderen nicht mitgeteilt werden. § 88 Abs. 4 gilt entsprechend. Das Abhören oder die in vergleichbarer Weise erfolgende Kenntnisnahme und die Weitergabe von Nachrichten auf Grund besonderer gesetzlicher Ermächtigung bleiben unberührt.

§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen

(1) Es ist verboten, Sendeanlagen oder sonstige Telekommunikationsanlagen zu besitzen, herzustellen, zu vertreiben, einzuführen oder sonst in den Geltungsbereich dieses Gesetzes zu verbringen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und auf Grund dieser Umstände oder auf Grund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen. Das Verbot, solche Anlagen zu besitzen, gilt nicht für denjenigen, der die tatsächliche Gewalt über eine solche Anlage

1. als Organ, als Mitglied eines Organs, als gesetzlicher Vertreter oder als vertretungsberechtigter Gesellschafter eines Berechtigten nach Absatz 2 erlangt,

2. von einem anderen oder für einen anderen Berechtigten nach Absatz 2 erlangt, sofern und solange er die Weisungen des anderen über die Ausübung der tatsächlichen Gewalt über die Anlage auf Grund eines Dienst- oder Arbeitsverhältnisses zu befolgen hat oder die tatsächliche Gewalt auf Grund gerichtlichen oder behördlichen Auftrags ausübt,

3. als Gerichtsvollzieher oder Vollzugsbeamter in einem Vollstreckungsverfahren erwirbt,

4. von einem Berechtigten nach Absatz 2 vorübergehend zum Zwecke der sicheren Verwahrung oder der nicht gewerbsmäßigen Beförderung zu einem Berechtigten erlangt,

5. lediglich zur gewerbsmäßigen Beförderung oder gewerbsmäßigen Lagerung erlangt,

6. durch Fund erlangt, sofern er die Anlage unverzüglich dem Verlierer, dem Eigentümer, einem sonstigen Erwerbsberechtigten oder der für die Entgegennahme der Fundanzeige zuständigen Stelle abliefert,

7. von Todes wegen erwirbt, sofern er die Anlage unverzüglich einem Berechtigten überlässt oder sie für dauernd unbrauchbar macht,

8. erlangt, die durch Entfernen eines wesentlichen Bauteils dauernd unbrauchbar gemacht worden ist, sofern er den Erwerb unverzüglich der Bundesnetzagentur schriftlich anzeigt, dabei seine Personalien, die Art der Anlage, deren Hersteller- oder Warenzeichen und, wenn die Anlage eine Herstellungsnummer hat, auch diese angibt sowie glaubhaft macht, dass er die Anlage ausschließlich zu Sammlerzwecken erworben hat.

(2) Die zuständigen obersten Bundes- oder Landesbehörden lassen Ausnahmen zu, wenn es im öffentlichen Interesse, insbesondere aus Gründen der öffentlichen Sicherheit, erforderlich ist. Absatz 1 Satz 1 gilt nicht, soweit das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) die Ausfuhr der Sendeanlagen oder sonstigen Telekommunikationsanlagen genehmigt hat.

(3) Es ist verboten, öffentlich oder in Mitteilungen, die für einen größeren Personenkreis bestimmt sind, für Sendeanlagen oder sonstige Telekommunikationsanlagen mit dem Hinweis zu werben, dass sie geeignet sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder dessen Bild von diesem unbemerkt aufzunehmen.

Abschnitt 2 Datenschutz

§ 91 Anwendungsbereich

(1) Dieser Abschnitt regelt den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken. Dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft, sofern sie mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, stehen den personenbezogenen Daten gleich.

(2) Für geschlossene Benutzergruppen öffentlicher Stellen der Länder gilt dieser Abschnitt mit der Maßgabe, dass an die Stelle des Bundesdatenschutzgesetzes die jeweiligen Landesdatenschutzgesetze treten.

§ 92 (weggefallen)

§ 93 Informationspflichten

(1) Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten so zu unterrichten, dass

die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Dabei sind die Teilnehmer auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Nutzer sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten. Das Auskunftsrecht nach dem Bundesdatenschutzgesetz bleibt davon unberührt.

(2) Unbeschadet des Absatzes 1 hat der Diensteanbieter in den Fällen, in denen ein besonderes Risiko der Verletzung der Netzsicherheit besteht, die Teilnehmer über dieses Risiko und, wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahme liegt, über mögliche Abhilfen, einschließlich der für sie voraussichtlich entstehenden Kosten, zu unterrichten.

(3) Im Fall einer Verletzung des Schutzes personenbezogener Daten haben die betroffenen Teilnehmer oder Personen die Rechte aus § 109a Absatz 1 Satz 2 in Verbindung mit Absatz 2.

§ 94 Einwilligung im elektronischen Verfahren

Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. der Teilnehmer oder Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Teilnehmer oder Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Teilnehmer oder Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

§ 95 Vertragsverhältnisse

(1) Der Diensteanbieter darf Bestandsdaten erheben und verwenden, soweit dieses zur Erreichung des in § 3 Nr. 3 genannten Zweckes erforderlich ist. Im Rahmen eines Vertragsverhältnisses mit einem anderen Diensteanbieter darf der Diensteanbieter Bestandsdaten seiner Teilnehmer und der Teilnehmer des anderen Diensteanbieters erheben und verwenden, soweit dies zur Erfüllung des Vertrages zwischen den Diensteanbietern erforderlich ist. Eine Übermittlung der Bestandsdaten an Dritte erfolgt, soweit nicht dieser Teil oder ein anderes Gesetz sie zulässt, nur mit Einwilligung des Teilnehmers.

(2) Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, zur Werbung für eigene Angebote, zur Marktforschung und zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers nur

verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. Ein Diensteanbieter, der im Rahmen einer bestehenden Kundenbeziehung rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers erhalten hat, darf diese für die Versendung von Text- oder Bildmitteilungen an ein Telefon oder an eine Postadresse zu den in Satz 1 genannten Zwecken verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann.

(3) Endet das Vertragsverhältnis, sind die Bestandsdaten vom Diensteanbieter mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. § 35 Abs. 3 des Bundesdatenschutzgesetzes gilt entsprechend.

(4) Der Diensteanbieter kann im Zusammenhang mit dem Begründen und dem Ändern des Vertragsverhältnisses sowie dem Erbringen von Telekommunikationsdiensten die Vorlage eines amtlichen Ausweises verlangen, wenn dies zur Überprüfung der Angaben des Teilnehmers erforderlich ist. Die Pflicht nach § 111 Absatz 1 Satz 3 bleibt unberührt. Er kann von dem Ausweis eine Kopie erstellen. Die Kopie ist vom Diensteanbieter unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Teilnehmers zu vernichten. Andere als die nach Absatz 1 zulässigen Daten darf der Diensteanbieter dabei nicht verwenden.

(5) Die Erbringung von Telekommunikationsdiensten darf nicht von einer Einwilligung des Teilnehmers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden, wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten ohne die Einwilligung nicht oder in nicht zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

§ 96 Verkehrsdaten

(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt genannten Zwecke erforderlich ist:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,

2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,

3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,

4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,

5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

Diese Verkehrsdaten dürfen nur verwendet werden, soweit dies für die in Satz 1 genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen erforderlich ist. *3*Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.

(2) Eine über Absatz 1 hinausgehende Erhebung oder Verwendung der Verkehrsdaten ist unzulässig.

(3) Der Diensteanbieter darf teilnehmerbezogene Verkehrsdaten, die vom Anbieter eines öffentlich zugänglichen Telekommunikationsdienstes verwendet werden, zum Zwecke der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und im dazu erforderlichen Zeitraum nur verwenden, sofern der Betroffene in diese Verwendung eingewilligt hat. Die Daten der Angerufenen sind unverzüglich zu anonymisieren. Eine zielnummernbezogene Verwendung der Verkehrsdaten durch den Diensteanbieter zu den in Satz 1 genannten Zwecken ist nur mit Einwilligung der Angerufenen zulässig. Hierbei sind die Daten der Anrufenden unverzüglich zu anonymisieren.

(4) Bei der Einholung der Einwilligung ist dem Teilnehmer mitzuteilen, welche Datenarten für die in Absatz 3 Satz 1 genannten Zwecke verarbeitet werden sollen und wie lange sie gespeichert werden sollen. Außerdem ist der Teilnehmer darauf hinzuweisen, dass er die Einwilligung jederzeit widerrufen kann.

§ 97 Entgeltermittlung und Entgeltabrechnung

(1) Diensteanbieter dürfen die in § 96 Abs. 1 aufgeführten Verkehrsdaten verwenden, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Teilnehmern benötigt werden. Erbringt ein Diensteanbieter seine Dienste über ein öffentliches Telekommunikationsnetz eines fremden Betreibers, darf der Betreiber des öffentlichen Telekommunikationsnetzes dem Diensteanbieter die für die Erbringung von dessen Diensten erhobenen Verkehrsdaten übermitteln. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er dem Dritten die in Absatz 2 genannten Daten übermitteln, soweit es zum Einzug des Entgelts und der Erstellung einer detaillierten Rechnung erforderlich ist. Der Dritte ist vertraglich zur Wahrung des Fernmeldegeheimnisses

nach § 88 und des Datenschutzes nach den §§ 93 und 95 bis 97, 99 und 100 zu verpflichten. § 11 des Bundesdatenschutzgesetzes bleibt unberührt.

(2) Der Diensteanbieter darf zur ordnungsgemäßen Ermittlung und Abrechnung der Entgelte für Telekommunikationsdienste und zum Nachweis der Richtigkeit derselben folgende personenbezogene Daten nach Maßgabe der Absätze 3 bis 6 erheben und verwenden:

1. die Verkehrsdaten nach § 96 Abs. 1,

2. die Anschrift des Teilnehmers oder Rechnungsempfängers, die Art des Anschlusses, die Zahl der im Abrechnungszeitraum einer planmäßigen Entgeltabrechnung insgesamt aufgekommenen Entgelteinheiten, die übermittelten Datenmengen, das insgesamt zu entrichtende Entgelt,

3. sonstige für die Entgeltabrechnung erhebliche Umstände wie Vorschusszahlungen, Zahlungen mit Buchungsdatum, Zahlungsrückstände, Mahnungen, durchgeführte und aufgehobene Anschlusssperren, eingereichte und bearbeitete Reklamationen, beantragte und genehmigte Stundungen, Ratenzahlungen und Sicherheitsleistungen.

(3) Der Diensteanbieter hat nach Beendigung der Verbindung aus den Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 3 und 5 unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

(4) Soweit es für die Abrechnung des Diensteanbieters mit anderen Diensteanbietern oder mit deren Teilnehmern sowie anderer Diensteanbieter mit ihren Teilnehmern erforderlich ist, darf der Diensteanbieter Verkehrsdaten verwenden.

(5) Zieht der Diensteanbieter mit der Rechnung Entgelte für Leistungen eines Dritten ein, die dieser im Zusammenhang mit der Erbringung von Telekommunikationsdiensten erbracht hat, so darf er dem Dritten Bestands- und Verkehrsdaten übermitteln, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Teilnehmer erforderlich sind.

§ 98 Standortdaten

(1) Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet werden, dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden

oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat. In diesen Fällen hat der Anbieter des Dienstes mit Zusatznutzen bei jeder Feststellung des Standortes des Mobilfunkendgerätes den Nutzer durch eine Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurden, zu informieren. Dies gilt nicht, wenn der Standort nur auf dem Endgerät angezeigt wird, dessen Standortdaten ermittelt wurden. Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 seine Einwilligung ausdrücklich, gesondert und schriftlich gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilen. In diesem Fall gilt die Verpflichtung nach Satz 2 entsprechend für den Anbieter des Dienstes mit Zusatznutzen. Der Anbieter des Dienstes mit Zusatznutzen darf die erforderlichen Bestandsdaten zur Erfüllung seiner Verpflichtung aus Satz 2 nutzen. Der Teilnehmer muss Mitbenutzer über eine erteilte Einwilligung unterrichten. Eine Einwilligung kann jederzeit widerrufen werden.

(2) Haben die Teilnehmer ihre Einwilligung zur Verarbeitung von Standortdaten gegeben, müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen.

(3) Bei Verbindungen zu Anschlüssen, die unter den Notrufnummern 112 oder 110 oder der Rufnummer 124 124 oder 116 117 erreicht werden, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Übermittlung von Standortdaten ausgeschlossen wird.

(4) Die Verarbeitung von Standortdaten nach den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

§ 99 Einzelverbindungsnachweis

(1) Dem Teilnehmer sind die gespeicherten Daten derjenigen Verbindungen, für die er entgeltpflichtig ist, nur dann mitzuteilen, wenn er vor dem maßgeblichen Abrechnungszeitraum in Textform einen Einzelverbindungsnachweis verlangt hat; auf Wunsch dürfen ihm auch die Daten pauschal abgegoltener Verbindungen mitgeteilt werden. Dabei entscheidet der Teilnehmer, ob ihm die von ihm gewählten Rufnummern ungekürzt oder unter Kürzung um die letzten drei Ziffern mitgeteilt werden. Bei Anschlüssen im Haushalt ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber informiert hat und künftige Mitbenutzer unverzüglich darüber informieren wird, dass ihm die Verkehrsdaten zur Erteilung des Nachweises

bekannt gegeben werden. Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. Soweit die öffentlich-rechtlichen Religionsgesellschaften für ihren Bereich eigene Mitarbeitervertreterregelungen erlassen haben, findet Satz 4 mit der Maßgabe Anwendung, dass an die Stelle des Betriebsrates oder der Personalvertretung die jeweilige Mitarbeitervertretung tritt. Dem Teilnehmer dürfen darüber hinaus die gespeicherten Daten mitgeteilt werden, wenn er Einwendungen gegen die Höhe der Verbindungsentgelte erhoben hat. Soweit ein Teilnehmer zur vollständigen oder teilweisen Übernahme der Entgelte für Verbindungen verpflichtet ist, die bei seinem Anschluss ankommen, dürfen ihm in dem für ihn bestimmten Einzelverbindungsnachweis die Nummern der Anschlüsse, von denen die Anrufe ausgehen, nur unter Kürzung um die letzten drei Ziffern mitgeteilt werden. Die Sätze 2 und 7 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

(2) Der Einzelverbindungsnachweis nach Absatz 1 Satz 1 darf nicht Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen erkennen lassen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen. Dies gilt nur, soweit die Bundesnetzagentur die angerufenen Anschlüsse in eine Liste aufgenommen hat. Der Beratung im Sinne des Satzes 1 dienen neben den in § 203 Absatz 1 Nummer 4 und 5 des Strafgesetzbuches genannten Personengruppen insbesondere die Telefonseelsorge und die Gesundheitsberatung. Die Bundesnetzagentur nimmt die Inhaber der Anschlüsse auf Antrag in die Liste auf, wenn sie ihre Aufgabenbestimmung nach Satz 1 durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts nachgewiesen haben. Die Liste wird zum Abruf im automatisierten Verfahren bereitgestellt. Der Diensteanbieter hat die Liste quartalsweise abzufragen und Änderungen unverzüglich in seinen Abrechnungsverfahren anzuwenden. Die Sätze 1 bis 6 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

(3) Bei Verwendung einer Kundenkarte muss auch auf der Karte ein deutlicher Hinweis auf die mögliche Mitteilung der gespeicherten Verkehrsdaten ersichtlich sein. Sofern ein solcher Hinweis auf der Karte aus technischen Gründen nicht möglich oder für den Kartenemittenten unzumutbar ist, muss der Teilnehmer eine Erklärung nach Absatz 1 Satz 3 oder Satz 4 abgegeben haben.

§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Die Kommunikationsinhalte sind nicht Bestandteil der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Die Daten sind unverzüglich zu löschen, sobald sie für die Beseitigung der Störung nicht mehr erforderlich sind. Eine Nutzung der Daten zu anderen Zwecken ist unzulässig. Soweit die Daten nicht automatisiert erhoben und verwendet werden, muss der betriebliche Datenschutzbeauftragte unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden. Der Diensteanbieter muss dem betrieblichen Datenschutzbeauftragten, der Bundesnetzagentur und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 6 in diesem Zeitraum schriftlich berichten. Die Bundesnetzagentur leitet diese Informationen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. Der Betroffene ist von dem Diensteanbieter zu benachrichtigen, sofern dieser ermittelt werden kann. Wurden im Rahmen einer Maßnahme nach Satz 1 auch Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung erhoben und verwendet, müssen die Berichte mindestens auch Angaben zum Umfang und zur Erforderlichkeit der Erhebung und Verwendung der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung enthalten.

(2) Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber der Telekommunikationsanlage oder seinem Beauftragten das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist. Eventuelle bei der Aufschaltung erstellte Aufzeichnungen sind unverzüglich zu löschen. Das Aufschalten muss den betroffenen Kommunikationsteilnehmern durch ein akustisches oder sonstiges Signal zeitgleich angezeigt und ausdrücklich mitgeteilt werden. Sofern dies technisch nicht möglich ist, muss der betriebliche Datenschutzbeauftragte unverzüglich detailliert über die Verfahren und Umstände jeder einzelnen Maßnahme informiert werden. Diese Informationen sind beim betrieblichen Datenschutzbeauftragten für zwei Jahre aufzubewahren.

(3) Wenn zu dokumentierende tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme eines Telekommunikationsnetzes oder -dienstes vorliegen, insbesondere für eine Leistungserschleichung oder einen Betrug, darf der Diensteanbieter zur Sicherung seines Entgeltanspruchs die Bestandsdaten und Verkehrsdaten verwenden, die erforderlich sind, um die rechtswidrige Inanspruchnahme des Telekommunikationsnetzes oder -dienstes aufzudecken und zu unterbinden. Der Diensteanbieter darf die nach § 96 erhobenen Verkehrsdaten in der Weise verwenden, dass aus dem Gesamtbestand aller Verkehrsdaten, die nicht älter als sechs Monate sind, die Daten derjenigen Verbindungen des Netzes ermittelt werden, für die tatsächliche Anhaltspunkte den Verdacht der rechtswidrigen Inanspruchnahme von Telekommunikationsnetzen und -diensten begründen. Der Diensteanbieter darf aus den Verkehrsdaten und Bestandsdaten nach Satz 1 einen pseudonymisierten Gesamtdatenbestand bilden, der Aufschluss über die von einzelnen Teilnehmern erzielten Umsätze gibt und unter Zugrundelegung geeigneter Kriterien das Auffinden solcher Verbindungen des Netzes ermöglicht, bei denen der Verdacht einer rechtswidrigen Inanspruchnahme besteht. Die Daten anderer Verbindungen sind unverzüglich zu löschen. Die Bundesnetzagentur und der Bundesbeauftragte für den Datenschutz sind über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.

(4) Unter den Voraussetzungen des Absatzes 3 Satz 1 darf der Diensteanbieter im Einzelfall Steuersignale erheben und verwenden, soweit dies zum Aufklären und Unterbinden der dort genannten Handlungen unerlässlich ist. Die Erhebung und Verwendung von anderen Nachrichteninhalten ist unzulässig. Über Einzelmaßnahmen nach Satz 1 ist die Bundesnetzagentur in Kenntnis zu setzen. Die Betroffenen sind zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahmen möglich ist.

§ 101 Mitteilen ankommender Verbindungen

(1) Trägt ein Teilnehmer in einem zu dokumentierenden Verfahren schlüssig vor, dass bei seinem Anschluss bedrohende oder belästigende Anrufe ankommen, hat der Diensteanbieter auf schriftlichen Antrag auch netzübergreifend Auskunft über die Inhaber der Anschlüsse zu erteilen, von denen die Anrufe ausgehen. Die Auskunft darf sich nur auf Anrufe beziehen, die nach Stellung des Antrags durchgeführt werden. Der Diensteanbieter darf die Rufnummern, Namen und Anschriften der Inhaber dieser Anschlüsse sowie Datum und Uhrzeit des Beginns der Verbindungen und der Verbindungsversuche erheben und verwenden sowie diese Daten seinem Teilnehmer mitteilen. Die Sätze 1 und 2 gelten nicht für Diensteanbieter, die ihre Dienste nur den Teilnehmern geschlossener Benutzergruppen anbieten.

(2) Die Bekanntgabe nach Absatz 1 Satz 3 darf nur erfolgen, wenn der Teilnehmer zuvor die Verbindungen nach Datum, Uhrzeit oder anderen geeigneten Kriterien eingrenzt, soweit ein Missbrauch dieses Verfahrens nicht auf andere Weise ausgeschlossen werden kann.

(3) Im Falle einer netzübergreifenden Auskunft sind die an der Verbindung mitwirkenden anderen Diensteanbieter verpflichtet, dem Diensteanbieter des bedrohten oder belästigten Teilnehmers die erforderlichen Auskünfte zu erteilen, sofern sie über diese Daten verfügen.

(4) Der Inhaber des Anschlusses, von dem die festgestellten Verbindungen ausgegangen sind, ist zu unterrichten, dass über diese Auskunft erteilt wurde. Davon kann abgesehen werden, wenn der Antragsteller schriftlich schlüssig vorgetragen hat, dass ihm aus dieser Mitteilung wesentliche Nachteile entstehen können, und diese Nachteile bei Abwägung mit den schutzwürdigen Interessen der Anrufenden als wesentlich schwerwiegender erscheinen. Erhält der Teilnehmer, von dessen Anschluss die als bedrohend oder belästigend bezeichneten Anrufe ausgegangen sind, auf andere Weise Kenntnis von der Auskunftserteilung, so ist er auf Verlangen über die Auskunftserteilung zu unterrichten.

(5) Die Bundesnetzagentur sowie der oder die Bundesbeauftragte für den Datenschutz sind über die Einführung und Änderung des Verfahrens zur Sicherstellung der Absätze 1 bis 4 unverzüglich in Kenntnis zu setzen.

§ 102 Rufnummernanzeige und -unterdrückung

(1) Bietet der Diensteanbieter die Anzeige der Rufnummer der Anrufenden an, so müssen Anrufende und Angerufene die Möglichkeit haben, die Rufnummernanzeige dauernd oder für jeden Anruf einzeln auf einfache Weise und unentgeltlich zu unterdrücken. Angerufene müssen die Möglichkeit haben, eingehende Anrufe, bei denen die Rufnummernanzeige durch den Anrufenden unterdrückt wurde, auf einfache Weise und unentgeltlich abzuweisen.

(2) Abweichend von Absatz 1 Satz 1 dürfen Anrufende bei Werbung mit einem Telefonanruf ihre Rufnummernanzeige nicht unterdrücken oder bei dem Diensteanbieter veranlassen, dass diese unterdrückt wird; der Anrufer hat sicherzustellen, dass dem Angerufenen die dem Anrufer zugeteilte Rufnummer übermittelt wird.

(3) Die Absätze 1 und 2 gelten nicht für Diensteanbieter, die ihre Dienste nur den Teilnehmern geschlossener Benutzergruppen anbieten.

(4) Auf Antrag des Teilnehmers muss der Diensteanbieter Anschlüsse bereitstellen, bei denen die Übermittlung der Rufnummer des Anschlusses, von dem der Anruf ausgeht, an den angerufenen Anschluss unentgeltlich ausgeschlossen ist. Die Anschlüsse sind auf Antrag des Teilnehmers in dem öffentlichen Teilnehmerverzeichnis (§ 104) seines Diensteanbieters zu kennzeichnen. Ist eine Kennzeichnung nach Satz 2 erfolgt, so darf an den so gekennzeichneten Anschluss eine Übermittlung der Rufnummer des Anschlusses, von dem der Anruf ausgeht, erst dann erfolgen, wenn zuvor die Kennzeichnung in der aktualisierten Fassung des Teilnehmerverzeichnisses nicht mehr enthalten ist.

(5) Hat der Teilnehmer die Eintragung in das Teilnehmerverzeichnis nicht nach § 104 beantragt, unterbleibt die Anzeige seiner Rufnummer bei dem angerufenen Anschluss, es sei denn, dass der Teilnehmer die Übermittlung seiner Rufnummer ausdrücklich wünscht.

(6) Wird die Anzeige der Rufnummer von Angerufenen angeboten, so müssen Angerufene die Möglichkeit haben, die Anzeige ihrer Rufnummer beim Anrufenden auf einfache Weise und unentgeltlich zu unterdrücken. Absatz 3 gilt entsprechend.

(7) Die Absätze 1 bis 3 und 6 gelten auch für Anrufe in das Ausland und für aus dem Ausland kommende Anrufe, soweit sie Anrufende oder Angerufene im Inland betreffen.

(8) Bei Verbindungen zu Anschlüssen, die unter den Notrufnummern 112 oder 110 oder der Rufnummer 124 124 oder 116 117 erreicht werden, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Anzeige von Nummern der Anrufenden ausgeschlossen wird.

§ 103 Automatische Anrufweiterschaltung

Der Diensteanbieter ist verpflichtet, seinen Teilnehmern die Möglichkeit einzuräumen, eine von einem Dritten veranlasste automatische Weiterschaltung auf sein Endgerät auf einfache Weise und unentgeltlich abzustellen, soweit dies technisch möglich ist. Satz 1 gilt nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

§ 104 Teilnehmerverzeichnisse

Teilnehmer können mit ihrem Namen, ihrer Anschrift und zusätzlichen Angaben wie Beruf, Branche und Art des Anschlusses in öffentliche gedruckte oder elektronische Verzeichnisse eingetragen werden, soweit sie dies beantragen. Dabei können die Teilnehmer bestimmen, welche Angaben in den Verzeichnissen veröffentlicht werden sollen. Auf Verlangen des Teilnehmers dürfen Mitbenutzer eingetragen werden, soweit diese damit einverstanden sind.

§ 105 Auskunftserteilung

(1) Über die in Teilnehmerverzeichnissen enthaltenen Rufnummern dürfen Auskünfte unter Beachtung der Beschränkungen des § 104 und der Absätze 2 und 3 erteilt werden.

(2) Die Telefonauskunft über Rufnummern von Teilnehmern darf nur erteilt werden, wenn diese in angemessener Weise darüber informiert worden sind, dass sie der Weitergabe ihrer Rufnummer widersprechen können und von ihrem Widerspruchsrecht keinen Gebrauch gemacht haben. Über Rufnummern hinausgehende Auskünfte über nach § 104 veröffentlichte Daten dürfen nur erteilt werden, wenn der Teilnehmer in eine weitergehende Auskunftserteilung eingewilligt hat.

(3) Die Telefonauskunft von Namen oder Namen und Anschrift eines Teilnehmers, von dem nur die Rufnummer bekannt ist, ist zulässig, wenn der Teilnehmer, der in ein Teilnehmerverzeichnis eingetragen ist, nach einem Hinweis seines Diensteanbieters auf seine Widerspruchsmöglichkeit nicht widersprochen hat.

(4) Ein Widerspruch nach Absatz 2 Satz 1 oder Absatz 3 oder eine Einwilligung nach Absatz 2 Satz 2 sind in den Kundendateien des Diensteanbieters und des Anbieters nach Absatz 1, die den Verzeichnissen zugrunde liegen, unverzüglich zu vermerken. Sie sind auch von den anderen Diensteanbietern zu beachten, sobald diese in zumutbarer Weise Kenntnis darüber erlangen konnten, dass der Widerspruch oder die Einwilligung in den Verzeichnissen des Diensteanbieters und des Anbieters nach Absatz 1 vermerkt ist.

§ 106 Telegrammdienst

(1) Daten und Belege über die betriebliche Bearbeitung und Zustellung von Telegrammen dürfen gespeichert werden, soweit es zum Nachweis einer ordnungsgemäßen Erbringung der Telegrammdienstleistung nach Maßgabe des mit dem Teilnehmer geschlossenen Vertrags erforderlich ist. Die Daten und Belege sind spätestens nach sechs Monaten vom Diensteanbieter zu löschen.

(2) Daten und Belege über den Inhalt von Telegrammen dürfen über den Zeitpunkt der Zustellung hinaus nur gespeichert werden, soweit der Diensteanbieter nach Maßgabe des mit dem Teilnehmer geschlossenen Vertrags für Übermittlungsfehler einzustehen hat. Bei Inlandstelegrammen sind die Daten und Belege spätestens nach drei Monaten, bei Auslandstelegrammen spätestens nach sechs Monaten vom Diensteanbieter zu löschen.

(3) Die Löschungsfristen beginnen mit dem ersten Tag des Monats, der auf den Monat der Telegrammaufgabe folgt. Die Löschung darf unterbleiben, solange die Verfolgung von Ansprüchen oder eine internationale Vereinbarung eine längere Speicherung erfordert.

§ 107 Nachrichtenübermittlungssysteme mit Zwischenspeicherung

(1) Der Diensteanbieter darf bei Diensten, für deren Durchführung eine Zwischenspeicherung erforderlich ist, Nachrichteninhalte, insbesondere Sprach-, Ton-, Text- und Grafikmitteilungen von Teilnehmern, im Rahmen eines hierauf gerichteten Diensteangebots unter folgenden Voraussetzungen verarbeiten:

1. Die Verarbeitung erfolgt ausschließlich in Telekommunikationsanlagen des zwischenspeichernden Diensteanbieters, es sei denn, die Nachrichteninhalte werden im Auftrag des Teilnehmers oder durch Eingabe des Teilnehmers in Telekommunikationsanlagen anderer Diensteanbieter weitergeleitet.

2. Ausschließlich der Teilnehmer bestimmt durch seine Eingabe Inhalt, Umfang und Art der Verarbeitung.

3. Ausschließlich der Teilnehmer bestimmt, wer Nachrichteninhalte eingeben und darauf zugreifen darf (Zugriffsberechtigter).

4. Der Diensteanbieter darf dem Teilnehmer mitteilen, dass der Empfänger auf die Nachricht zugegriffen hat.

5. Der Diensteanbieter darf Nachrichteninhalte nur entsprechend dem mit dem Teilnehmer geschlossenen Vertrag löschen.

(2) Der Diensteanbieter hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten innerhalb seines Unternehmens oder an Dritte auszuschließen. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Soweit es im Hinblick auf den angestrebten Schutzzweck erforderlich ist, sind die Maßnahmen dem jeweiligen Stand der Technik anzupassen.

Abschnitt 3 Öffentliche Sicherheit

§ 108 Notruf

(1) Wer öffentlich zugängliche Telekommunikationsdienste für das Führen von ausgehenden Inlandsgesprächen zu einer oder mehreren Nummern des nationalen Telefonnummernplanes bereitstellt, hat Vorkehrungen zu treffen, damit Endnutzern unentgeltliche Verbindungen möglich sind, die entweder durch die Wahl der europaeinheitlichen Notrufnummer 112 oder der zusätzlichen nationalen Notrufnummer 110 oder durch das Aussenden entsprechender Signalisierungen eingeleitet werden (Notrufverbindungen). Wer derartige öffentlich zugängliche Telekommunikationsdienste erbringt, den Zugang zu solchen Diensten ermöglicht oder Telekommunikationsnetze betreibt, die für diese Dienste einschließlich der Durchleitung von Anrufen genutzt werden, hat gemäß Satz 4 sicherzustellen oder im notwendigen Umfang daran mitzuwirken, dass Notrufverbindungen unverzüglich zu der örtlich zuständigen Notrufabfragestelle hergestellt werden, und er hat alle erforderlichen Maßnahmen zu treffen, damit Notrufverbindungen jederzeit möglich sind. Die Diensteanbieter nach den Sätzen 1 und 2 haben gemäß Satz 6 sicherzustellen, dass der Notrufabfragestelle auch Folgendes mit der Notrufverbindung übermittelt wird:

1. die Rufnummer des Anschlusses, von dem die Notrufverbindung ausgeht, und

2. die Daten, die zur Ermittlung des Standortes erforderlich sind, von dem die Notrufverbindung ausgeht.

Notrufverbindungen sind vorrangig vor anderen Verbindungen herzustellen, sie stehen vorrangigen Verbindungen nach dem Post- und Telekommunikationssicherstellungsgesetz gleich. Daten, die nach Maßgabe der Rechtsverordnung nach Absatz 3 zur Verfolgung von Missbrauch des Notrufs erforderlich sind, dürfen auch verzögert an die Notrufabfragestelle übermittelt werden. Die Übermittlung der Daten nach den Sätzen 3 und 5 erfolgt unentgeltlich. Die für Notrufverbindungen entstehenden Kosten trägt jeder Diensteanbieter selbst; die Entgeltlichkeit von Vorleistungen bleibt unberührt.

(2) Im Hinblick auf Notrufverbindungen, die durch sprach- oder hörbehinderte Endnutzer unter Verwendung eines Telefaxgerätes eingeleitet werden, gilt Absatz 1 entsprechend.

(3) Das Bundesministerium für Wirtschaft und Energie wird ermächtigt, im Einvernehmen mit dem Bundesministerium des Innern, dem Bundesministerium für Verkehr und digitale Infrastruktur und dem Bundesministerium für Arbeit und Soziales durch Rechtsverordnung mit Zustimmung des Bundesrates Regelungen zu treffen

1. zu den Grundsätzen der Festlegung von Einzugsgebieten von Notrufabfragestellen und deren Unterteilungen durch die für den Notruf zuständigen Landes- und Kommunalbehörden sowie zu den Grundsätzen des Abstimmungsverfahrens zwischen diesen Behörden und den betroffenen Teilnehmernetzbetreibern und Mobilfunknetzbetreibern, soweit diese Grundsätze für die Herstellung von Notrufverbindungen erforderlich sind,

2. zur Herstellung von Notrufverbindungen zur jeweils örtlich zuständigen Notrufabfragestelle oder Ersatznotrufabfragestelle,

3. zum Umfang der für Notrufverbindungen zu erbringenden Leistungsmerkmale, einschließlich

   a) der Übermittlung der Daten nach Absatz 1 Satz 3 und

   b) zulässiger Abweichungen hinsichtlich der nach Absatz 1 Satz 3 Nummer 1 zu übermittelnden Daten in unausweichlichen technisch bedingten Sonderfällen,

4. zur Bereitstellung und Übermittlung von Daten, die geeignet sind, der Notrufabfragestelle die Verfolgung von Missbrauch des Notrufs zu ermöglichen,

5. zum Herstellen von Notrufverbindungen mittels automatischer Wählgeräte und

6. zu den Aufgaben der Bundesnetzagentur auf den in den Nummern 1 bis 5 aufgeführten Gebieten, insbesondere im Hinblick auf die Festlegung von Kriterien für die Genauigkeit und Zuverlässigkeit der Daten, die zur Ermittlung des Standortes erforderlich sind, von dem die Notrufverbindung ausgeht.

Landesrechtliche Regelungen über Notrufabfragestellen bleiben von den Vorschriften dieses Absatzes insofern unberührt, als sie nicht Verpflichtungen im Sinne von Absatz 1 betreffen.

(4) Die technischen Einzelheiten zu den in Absatz 3 Satz 1 Nummer 1 bis 5 aufgeführten Gegenständen, insbesondere die Kriterien für die Genauigkeit und Zuverlässigkeit der Angaben zu dem Standort, von dem die Notrufverbindung ausgeht, legt die Bundesnetzagentur in einer Technischen Richtlinie fest; dabei berücksichtigt sie die Vorschriften der Verordnung nach Absatz 3. *2*Die Bundesnetzagentur erstellt die Richtlinie unter Beteiligung

1. der Verbände der durch Absatz 1 Satz 1 und 2 und Absatz 2 betroffenen Diensteanbieter und Betreiber von Telekommunikationsnetzen,

2. der vom Bundesministerium des Innern benannten Vertreter der Betreiber von Notrufabfragestellen und

3. der Hersteller der in den Telekommunikationsnetzen und Notrufabfragestellen eingesetzten technischen Einrichtungen.

Bei den Festlegungen in der Technischen Richtlinie sind internationale Standards zu berücksichtigen; Abweichungen von den Standards sind zu begründen. Die Technische Richtlinie ist von der Bundesnetzagentur auf ihrer Internetseite zu veröffentlichen; die Veröffentlichung hat die Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen. Die Verpflichteten nach Absatz 1 Satz 1 bis 3 und Absatz 2 haben die Anforderungen der Technischen Richtlinie spätestens ein Jahr nach deren Bekanntmachung zu erfüllen, sofern dort für bestimmte Verpflichtungen kein längerer Übergangszeitraum festgelegt ist. Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.

§ 109 Technische Schutzmaßnahmen

(1) Jeder Diensteanbieter hat erforderliche technische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz des Fernmeldegeheimnisses und

2. gegen die Verletzung des Schutzes personenbezogener Daten.

Dabei ist der Stand der Technik zu berücksichtigen.

(2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und

2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten.

   Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. Bei Maßnahmen nach Satz 2 ist der Stand der Technik zu berücksichtigen. Wer ein öffentliches Telekommunikationsnetz betreibt, hat Maßnahmen zu treffen, um den ordnungsgemäßen Betrieb seiner Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen. Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. § 11 Absatz 1 des Bundesdatenschutzgesetzes gilt entsprechend.

(3) Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Beteiligte die Verpflichtungen nach den Absätzen 1 und 2 zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Beteiligten zugeordnet werden können.

(4) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,

1. welches öffentliche Telekommunikationsnetz betrieben und welche öffentlich zugänglichen Telekommunikationsdienste erbracht werden,

2. von welchen Gefährdungen auszugehen ist und

3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind.

   Wer ein öffentliches Telekommunikationsnetz betreibt, hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach der Aufnahme des Netzbetriebs vorzulegen. Wer öffentlich zugängliche Telekommunikationsdienste erbringt, kann nach der Bereitstellung des Telekommunikationsdienstes von der Bundesnetzagentur verpflichtet werden, das Sicherheitskonzept vorzulegen. Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie deren unverzügliche Beseitigung verlangen. Sofern sich die dem Sicherheitskonzept zugrunde liegenden Gegebenheiten ändern, hat der nach Satz 2 oder 3 Verpflichtete das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen. Die Bundesnetzagentur überprüft regelmäßig die Umsetzung des Sicherheitskonzepts. Die Überprüfung soll mindestens alle zwei Jahre erfolgen.

(5) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die

1. zu beträchtlichen Sicherheitsverletzungen führen oder

2. zu beträchtlichen Sicherheitsverletzungen führen können.

Dies schließt Störungen ein, die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und zu der betroffenen Informationstechnik enthalten. Kommt es zu einer beträchtlichen Sicherheitsverletzung, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. § 8e des BSI-Gesetzes gilt entsprechend. Die Bundesnetzagentur legt der Europäischen Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen vor.

(6) Die Bundesnetzagentur erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach Absatz 4 und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach den Absätzen 1 und 2. Sie gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme. Der Katalog wird von der Bundesnetzagentur veröffentlicht.

(7) Die Bundesnetzagentur kann anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird, ob die Anforderungen nach den

Absätzen 1 bis 3 erfüllt sind. Der nach Satz 1 Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bundesnetzagentur zu übermitteln. Er trägt die Kosten dieser Überprüfung.

(8) Über aufgedeckte Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik.

§ 109a Daten- und Informationssicherheit

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen. Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden, hat der Anbieter des Telekommunikationsdienstes zusätzlich die Betroffenen unverzüglich von dieser Verletzung zu benachrichtigen. In Fällen, in denen in dem Sicherheitskonzept nachgewiesen wurde, dass die von der Verletzung betroffenen personenbezogenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden, ist eine Benachrichtigung nicht erforderlich. Unabhängig von Satz 3 kann die Bundesnetzagentur den Anbieter des Telekommunikationsdienstes unter Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten zu einer Benachrichtigung der Betroffenen verpflichten. Im Übrigen gilt § 42a Satz 6 des Bundesdatenschutzgesetzes entsprechend.

(2) Die Benachrichtigung an die Betroffenen muss mindestens enthalten:

1. die Art der Verletzung des Schutzes personenbezogener Daten,
2. Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind, und
3. Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen.

In der Benachrichtigung an die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat der Anbieter des Telekommunikationsdienstes zusätzlich zu den Angaben nach Satz 1 die Folgen der Verletzung des Schutzes personenbezogener Daten und die beabsichtigten oder ergriffenen Maßnahmen darzulegen.

(3) Die Anbieter der Telekommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, das Angaben zu Folgendem enthält:

1. zu den Umständen der Verletzungen,

2. zu den Auswirkungen der Verletzungen und

3. zu den ergriffenen Abhilfemaßnahmen.

Diese Angaben müssen ausreichend sein, um der Bundesnetzagentur und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Prüfung zu ermöglichen, ob die Bestimmungen der Absätze 1 und 2 eingehalten wurden. Das Verzeichnis enthält nur die zu diesem Zweck erforderlichen Informationen und muss nicht Verletzungen berücksichtigen, die mehr als fünf Jahre zurückliegen.

(4) Werden dem Diensteanbieter nach Absatz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können. Der Diensteanbieter darf die Teile des Datenverkehrs von und zu einem Nutzer, von denen eine Störung ausgeht, umleiten, soweit dies erforderlich ist, um den Nutzer über die Störungen benachrichtigen zu können.

(5) Der Diensteanbieter darf im Falle einer Störung die Nutzung des Telekommunikationsdienstes bis zur Beendigung der Störung einschränken, umleiten oder unterbinden, soweit dies erforderlich ist, um die Beeinträchtigung der Telekommunikations- und Datenverarbeitungssysteme des Diensteanbieters, eines Nutzers im Sinne des Absatzes 4 oder anderer Nutzer zu beseitigen oder zu verhindern und der Nutzer die Störung nicht unverzüglich selbst beseitigt oder zu erwarten ist, dass der Nutzer die Störung selbst nicht unverzüglich beseitigt.

(6) Der Diensteanbieter darf den Datenverkehr zu Störungsquellen einschränken oder unterbinden, soweit dies zur Vermeidung von Störungen in den Telekommunikations-und Datenverarbeitungssystemen der Nutzer erforderlich ist.

(7) Vorbehaltlich technischer Durchführungsmaßnahmen der Europäischen Kommission nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG kann die Bundesnetzagentur Leitlinien vorgeben bezüglich des Formats, der Verfahrensweise und der Umstände, unter denen eine Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist.

§ 110 Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften

(1) Wer eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, hat

1. ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen,

1a. in Fällen, in denen die Überwachbarkeit nur durch das Zusammenwirken von zwei oder mehreren Telekommunikationsanlagen sichergestellt werden kann, die dazu erforderlichen automatischen Steuerungsmöglichkeiten zur Erfassung und Ausleitung der zu überwachenden Telekommunikation in seiner Telekommunikationsanlage bereitzustellen sowie eine derartige Steuerung zu ermöglichen,

2. der Bundesnetzagentur unverzüglich nach der Betriebsaufnahme

   a) zu erklären, dass er die Vorkehrungen nach Nummer 1 getroffen hat sowie

   b) eine im Inland gelegene Stelle zu benennen, die für ihn bestimmte Anordnungen zur Überwachung der Telekommunikation entgegennimmt,

3. der Bundesnetzagentur den unentgeltlichen Nachweis zu erbringen, dass seine technischen Einrichtungen und organisatorischen Vorkehrungen nach Nummer 1 mit den Vorschriften der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 übereinstimmen; dazu hat er unverzüglich, spätestens nach einem Monat nach Betriebsaufnahme,

   a) der Bundesnetzagentur die Unterlagen zu übersenden, die dort für die Vorbereitung der im Rahmen des Nachweises von der Bundesnetzagentur durchzuführenden Prüfungen erforderlich sind, und

   b) mit der Bundesnetzagentur einen Prüftermin für die Erbringung dieses Nachweises zu vereinbaren;

   bei den für den Nachweis erforderlichen Prüfungen hat er die Bundesnetzagentur zu unterstützen,

4. der Bundesnetzagentur auf deren besondere Aufforderung im begründeten Einzelfall eine erneute unentgeltliche Prüfung seiner technischen und organisatorischen Vorkehrungen zu gestatten sowie

5. die Aufstellung und den Betrieb von Geräten für die Durchführung von Maßnahmen nach den §§ 5 und 8 des Artikel 10-Gesetzes oder nach den §§ 6, 12 und 14 des BND-Gesetzes in seinen Räumen zu dulden und Bediensteten der für diese Maßnahmen zuständigen Stelle sowie bei Maßnahmen nach den §§ 5 und 8 des Artikel 10-Gesetzes den Mitgliedern und Mitarbeitern der G 10-Kommission (§ 1 Abs. 2 des Artikel 10-Gesetzes) Zugang zu diesen Geräten zur Erfüllung ihrer gesetzlichen Aufgaben zu gewähren.

Wer öffentlich zugängliche Telekommunikationsdienste erbringt, ohne hierfür eine Telekommunikationsanlage zu betreiben, hat sich bei der Auswahl des Betreibers der dafür genutzten Telekommunikationsanlage zu vergewissern, dass dieser Anordnungen zur Überwachung der Telekommunikation unverzüglich nach Maßgabe der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 umsetzen kann und der Bundesnetzagentur unverzüglich nach Aufnahme seines Dienstes mitzuteilen, welche Telekommunikationsdienste er erbringt, durch wen Überwachungsanordnungen, die seine Teilnehmer betreffen, umgesetzt werden und an welche im Inland gelegene Stelle Anordnungen zur Überwachung der Telekommunikation zu richten sind. Änderungen der den Mitteilungen nach Satz 1 Nr. 2 Buchstabe b und Satz 2 zugrunde liegenden Daten sind der Bundesnetzagentur unverzüglich mitzuteilen. In Fällen, in denen noch keine Vorschriften nach Absatz 3 vorhanden sind, hat der Verpflichtete die technischen Einrichtungen nach Satz 1 Nr. 1 und 1a in Absprache mit der Bundesnetzagentur zu gestalten, die entsprechende Festlegungen im Benehmen mit den berechtigten Stellen trifft. Die Sätze 1 bis 4 gelten nicht, soweit die Rechtsverordnung nach Absatz 2 Ausnahmen für die Telekommunikationsanlage vorsieht. § 100b Abs. 3 Satz 1 der Strafprozessordnung, § 2 Abs. 1 Satz 3 des Artikel 10-Gesetzes, § 20l Abs. 5 Satz 1 des Bundeskriminalamtgesetzes, § 8 Absatz 1 Satz 1 des BND-Gesetzes sowie entsprechende landesgesetzliche Regelungen zur polizeilich-präventiven Telekommunikationsüberwachung bleiben unberührt.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates

1. Regelungen zu treffen

   a) über die grundlegenden technischen Anforderungen und die organisatorischen Eckpunkte für die Umsetzung von Überwachungsmaßnahmen und die Erteilung von Auskünften einschließlich der Umsetzung von Überwachungsmaßnahmen und der Erteilung von Auskünften durch einen von dem Verpflichteten beauftragten Erfüllungsgehilfen,

   b) über den Regelungsrahmen für die Technische Richtlinie nach Absatz 3,

   c) für den Nachweis nach Absatz 1 Satz 1 Nr. 3 und 4 und

   d) für die nähere Ausgestaltung der Duldungsverpflichtung nach Absatz 1 Satz 1 Nr. 5 sowie

2. zu bestimmen,

   a) in welchen Fällen und unter welchen Bedingungen vorübergehend auf die Einhaltung bestimmter technischer Vorgaben verzichtet werden kann,

   b) dass die Bundesnetzagentur aus technischen Gründen Ausnahmen von der Erfüllung einzelner technischer Anforderungen zulassen kann und

c) bei welchen Telekommunikationsanlagen und damit erbrachten Diensteangeboten aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit abweichend von Absatz 1 Satz 1 Nr. 1 keine technischen Einrichtungen vorgehalten und keine organisatorischen Vorkehrungen getroffen werden müssen.

(3) Die Bundesnetzagentur legt technische Einzelheiten, die zur Sicherstellung einer vollständigen Erfassung der zu überwachenden Telekommunikation und zur Auskunftserteilung sowie zur Gestaltung des Übergabepunktes zu den berechtigten Stellen erforderlich sind, in einer im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller zu erstellenden Technischen Richtlinie fest. Dabei sind internationale technische Standards zu berücksichtigen; Abweichungen von den Standards sind zu begründen. Die Technische Richtlinie ist von der Bundesnetzagentur auf ihrer Internetseite zu veröffentlichen; die Veröffentlichung hat die Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen.

(4) Wer technische Einrichtungen zur Umsetzung von Überwachungsmaßnahmen herstellt oder vertreibt, kann von der Bundesnetzagentur verlangen, dass sie diese Einrichtungen im Rahmen einer Typmusterprüfung im Zusammenwirken mit bestimmten Telekommunikationsanlagen daraufhin prüft, ob die rechtlichen und technischen Vorschriften der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 erfüllt werden. Die Bundesnetzagentur kann nach pflichtgemäßem Ermessen vorübergehend Abweichungen von den technischen Vorgaben zulassen, sofern die Umsetzung von Überwachungsmaßnahmen grundsätzlich sichergestellt ist und sich ein nur unwesentlicher Anpassungsbedarf bei den Einrichtungen der berechtigten Stellen ergibt. Die Bundesnetzagentur hat dem Hersteller oder Vertreiber das Prüfergebnis schriftlich mitzuteilen. Die Prüfergebnisse werden von der Bundesnetzagentur bei dem Nachweis der Übereinstimmung der technischen Einrichtungen mit den anzuwendenden technischen Vorschriften beachtet, den der Verpflichtete nach Absatz 1 Satz 1 Nr. 3 oder 4 zu erbringen hat. Die vom Bundesministerium für Wirtschaft und Technologie vor Inkrafttreten dieser Vorschrift ausgesprochenen Zustimmungen zu den von Herstellern vorgestellten Rahmenkonzepten gelten als Mitteilungen im Sinne des Satzes 3.

(5) Wer nach Absatz 1 in Verbindung mit der Rechtsverordnung nach Absatz 2 verpflichtet ist, Vorkehrungen zu treffen, hat die Anforderungen der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3 spätestens ein Jahr nach deren Bekanntmachung zu erfüllen, sofern dort für bestimmte Verpflichtungen kein längerer Zeitraum festgelegt ist. Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen für bereits vom Verpflichteten angebotene Telekommunikationsdienste müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen. Stellt sich bei dem Nachweis nach Absatz 1 Satz 1 Nr. 3 oder einer erneuten Prüfung nach Absatz 1 Satz 1 Nr. 4 ein Mangel bei den von dem Verpflichteten getroffenen technischen oder

organisatorischen Vorkehrungen heraus, hat er diesen Mangel nach Vorgaben der Bundesnetzagentur in angemessener Frist zu beseitigen; stellt sich im Betrieb, insbesondere anlässlich durchzuführender Überwachungsmaßnahmen, ein Mangel heraus, hat er diesen unverzüglich zu beseitigen. Sofern für die technische Einrichtung eine Typmusterprüfung nach Absatz 4 durchgeführt worden ist und dabei Fristen für die Beseitigung von Mängeln festgelegt worden sind, hat die Bundesnetzagentur diese Fristen bei ihren Vorgaben zur Mängelbeseitigung nach Satz 3 zu berücksichtigen.

(6) Jeder Betreiber einer Telekommunikationsanlage, der anderen im Rahmen seines Angebotes für die Öffentlichkeit Netzabschlusspunkte seiner Telekommunikationsanlage überlässt, ist verpflichtet, den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf deren Anforderung Netzabschlusspunkte für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen unverzüglich und vorrangig bereitzustellen. Die technische Ausgestaltung derartiger Netzabschlusspunkte kann in einer Rechtsverordnung nach Absatz 2 geregelt werden. Für die Bereitstellung und Nutzung gelten mit Ausnahme besonderer Tarife oder Zuschläge für vorrangige oder vorzeitige Bereitstellung oder Entstörung die jeweils für die Allgemeinheit anzuwendenden Tarife. Besondere vertraglich vereinbarte Rabatte bleiben von Satz 3 unberührt.

(7) Telekommunikationsanlagen, die von den gesetzlich berechtigten Stellen betrieben werden und mittels derer in das Fernmeldegeheimnis oder in den Netzbetrieb eingegriffen werden soll, sind im Einvernehmen mit der Bundesnetzagentur technisch zu gestalten. Die Bundesnetzagentur hat sich zu der technischen Gestaltung innerhalb angemessener Frist zu äußern.

(8) (weggefallen)

(9) (weggefallen)

§ 111 Daten für Auskunftsersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,

5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie

6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Bei im Voraus bezahlten Mobilfunkdiensten ist die Richtigkeit der nach Satz 1 erhobenen Daten vor der Freischaltung zu überprüfen durch

1. Vorlage eines Ausweises im Sinne des § 2 Absatz 1 des Personalausweisgesetzes,

2. Vorlage eines Passes im Sinne des § 1 Absatz 2 des Passgesetzes,

3. Vorlage eines sonstigen gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, wozu insbesondere auch ein nach ausländerrechtlichen Bestimmungen anerkannter oder zugelassener Pass, Personalausweis oder Pass- oder Ausweisersatz zählt,

4. Vorlage eines Aufenthaltstitels,

5. Vorlage eines Ankunftsnachweises nach § 63a Absatz 1 des Asylgesetzes oder einer Bescheinigung über die Aufenthaltsgestattung nach § 63 Absatz 1 des Asylgesetzes,

6. Vorlage einer Bescheinigung über die Aussetzung der Abschiebung nach § 60a Absatz 4 des Aufenthaltsgesetzes oder

7. Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den darin enthaltenen Daten, sofern es sich bei dem Anschlussinhaber um eine juristische Person oder Personengesellschaft handelt,

soweit die Daten in den vorgelegten Dokumenten oder eingesehenen Registern oder Verzeichnissen enthalten sind. Die Überprüfung kann auch durch andere geeignete Verfahren erfolgen; die Bundesnetzagentur legt nach Anhörung der betroffenen Kreise durch Verfügung im Amtsblatt fest, welche anderen Verfahren zur Überprüfung geeignet sind, wobei jeweils zum Zwecke der Identifikation vor Freischaltung der vertraglich vereinbarten Mobilfunkdienstleistung ein Dokument im Sinne des Satzes 3 genutzt werden muss. Bei der Überprüfung ist die Art des eingesetzten Verfahrens zu speichern; bei Überprüfung mittels eines Dokumentes im Sinne des Satzes 3 Nummer 1 bis 6 sind ferner Angaben zu Art, Nummer und ausstellender Stelle zu speichern. Für die Identifizierung anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Auf-

enthaltsgesetzes gilt § 8 Absatz 2 Satz 4 des Geldwäschegesetzes entsprechend. 7Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

(2) Die Verpflichtung zur unverzüglichen Speicherung nach Absatz 1 Satz 1 gilt hinsichtlich der Daten nach Absatz 1 Satz 1 Nummer 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Absatz 1 Satz 1 Nummer 1 und 2 erhebt, wobei an die Stelle der Daten nach Absatz 1 Satz 1 Nummer 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Absatz 1 Satz 1 Nummer 2 der Inhaber des elektronischen Postfachs tritt.

(3) Wird dem Verpflichteten nach Absatz 1 Satz 1 oder Absatz 2 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen. In diesem Zusammenhang hat der nach Absatz 1 Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist.

(4) Bedient sich ein Diensteanbieter zur Erhebung der Daten nach Absatz 1 Satz 1 und Absatz 2 eines Dritten, bleibt er für die Erfüllung der Pflichten nach Absatz 1 Satz 1 und Absatz 2 verantwortlich. Werden dem Dritten im Rahmen des üblichen Geschäftsablaufes Änderungen der Daten nach Absatz 1 Satz 1 und Absatz 2 bekannt, hat er diese dem Diensteanbieter unverzüglich zu übermitteln.

(5) Die Daten nach den Absätzen 1 und 2 sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(6) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

§ 112 Automatisiertes Auskunftsverfahren

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat die nach § 111 Absatz 1 Satz 1, Absatz 2, 3 und 4 erhobenen Daten unverzüglich in Kundendateien zu speichern, in die auch Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere Anbieter von Telekommunikationsdiensten vergeben werden, sowie bei portierten Rufnummern die aktuelle Portierungskennung aufzunehmen sind. Der Verpflichtete kann auch eine andere Stelle nach Maßgabe des § 11 des Bundesdatenschutzgesetzes beauftragen, die Kundendateien zu führen. Für die Berichtigung und Löschung der in den Kundendateien gespeicherten Daten gilt § 111 Absatz 3 und 5 entsprechend. In Fällen portierter Rufnummern sind die Rufnummer und die zugehörige Portierungskennung erst nach Ablauf des Jahres zu löschen, das dem Zeitpunkt folgt, zu dem die Rufnummer wieder an den Netzbetreiber zurückgegeben wurde, dem sie ursprünglich zugeteilt worden war. Der Verpflichtete hat zu gewährleisten, dass

1. die Bundesnetzagentur jederzeit Daten aus den Kundendateien automatisiert im Inland abrufen kann,

2. der Abruf von Daten unter Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichenfunktion erfolgen kann.

Der Verpflichtete und sein Beauftragter haben durch technische und organisatorische Maßnahmen sicherzustellen, dass ihnen Abrufe nicht zur Kenntnis gelangen können. Die Bundesnetzagentur darf Daten aus den Kundendateien nur abrufen, soweit die Kenntnis der Daten erforderlich ist

1. für die Verfolgung von Ordnungswidrigkeiten nach diesem Gesetz oder nach dem Gesetz gegen den unlauteren Wettbewerb,

2. für die Erledigung von Auskunftsersuchen der in Absatz 2 genannten Stellen.

Die ersuchende Stelle prüft unverzüglich, inwieweit sie die als Antwort übermittelten Daten benötigt, nicht benötigte Daten löscht sie unverzüglich; dies gilt auch für die Bundesnetzagentur für den Abruf von Daten nach Satz 7 Nummer 1.

(2) Auskünfte aus den Kundendateien nach Absatz 1 werden

1. den Gerichten und Strafverfolgungsbehörden,

2. den Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr,

3. dem Zollkriminalamt und den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 23a des Zollfahndungsdienstgesetzes,

4. den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst,

5. den Notrufabfragestellen nach § 108 sowie der Abfragestelle für die Rufnummer 124 124,

6. der Bundesanstalt für Finanzdienstleistungsaufsicht sowie

7. den Behörden der Zollverwaltung für die in § 2 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen

nach Absatz 4 jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen an die Bundesnetzagentur im automatisierten Verfahren vorgelegt werden.

(3) Das Bundesministerium für Wirtschaft und Energie wird ermächtigt, im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium des Innern, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundes-

ministerium für Verkehr und digitale Infrastruktur sowie dem Bundesministerium der Verteidigung eine Rechtsverordnung mit Zustimmung des Bundesrates zu erlassen, in der geregelt werden

1. die wesentlichen Anforderungen an die technischen Verfahren

   a) zur Übermittlung der Ersuchen an die Bundesnetzagentur,

   b) zum Abruf der Daten durch die Bundesnetzagentur von den Verpflichteten einschließlich der für die Abfrage zu verwendenden Datenarten und

   c) zur Übermittlung der Ergebnisse des Abrufs von der Bundesnetzagentur an die ersuchenden Stellen,

2. die zu beachtenden Sicherheitsanforderungen,

3. für Abrufe mit unvollständigen Abfragedaten und für die Suche mittels einer Ähnlichenfunktion

   a) die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung der gesuchten Person,

   b) die Zeichen, die in der Abfrage verwendet werden dürfen,

   c) Anforderungen an den Einsatz sprachwissenschaftlicher Verfahren, die gewährleisten, dass unterschiedliche Schreibweisen eines Personen-, Straßen- oder Ortsnamens sowie Abweichungen, die sich aus der Vertauschung, Auslassung oder Hinzufügung von Namensbestandteilen ergeben, in die Suche und das Suchergebnis einbezogen werden,

   d) die zulässige Menge der an die Bundesnetzagentur zu übermittelnden Antwortdatensätze sowie

4. wer abweichend von Absatz 1 Satz 1 aus Gründen der Verhältnismäßigkeit keine Kundendateien für das automatisierte Auskunftsverfahren vorhalten muss; in diesen Fällen gilt § 111 Absatz 1 Satz 7 entsprechend.

Im Übrigen können in der Verordnung auch Einschränkungen der Abfragemöglichkeit für die in Absatz 2 Nr. 5 bis 7 genannten Stellen auf den für diese Stellen erforderlichen Umfang geregelt werden. Die technischen Einzelheiten des automatisierten Abrufverfahrens gibt die Bundesnetzagentur in einer unter Beteiligung der betroffenen Verbände und der berechtigten Stellen zu erarbeitenden Technischen Richtlinie vor, die bei Bedarf an den Stand der Technik anzupassen und von der Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen ist. Der Verpflichtete nach Absatz 1 und die berechtigten Stellen haben die Anforderungen der Technischen Richtlinie spätestens ein Jahr nach deren Bekanntmachung zu erfüllen. Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen müssen im

Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.

(4) Auf Ersuchen der in Absatz 2 genannten Stellen hat die Bundesnetzagentur die entsprechenden Datensätze aus den Kundendateien nach Absatz 1 abzurufen und an die ersuchende Stelle zu übermitteln. Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlass besteht. Die Verantwortung für die Zulässigkeit der Übermittlung tragen

1. in den Fällen des Absatzes 1 Satz 7 Nummer 1 die Bundesnetzagentur und
2. in den Fällen des Absatzes 1 Satz 7 Nummer 2 die in Absatz 2 genannten Stellen.

Die Bundesnetzagentur protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum. Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig. Die Protokolldaten sind nach einem Jahr zu löschen.

(5) Der Verpflichtete nach Absatz 1 hat alle technischen Vorkehrungen in seinem Verantwortungsbereich auf seine Kosten zu treffen, die für die Erteilung der Auskünfte nach dieser Vorschrift erforderlich sind. Dazu gehören auch die Anschaffung der zur Sicherstellung der Vertraulichkeit und des Schutzes vor unberechtigten Zugriffen erforderlichen Geräte, die Einrichtung eines geeigneten Telekommunikationsanschlusses und die Teilnahme an dem geschlossenen Benutzersystem sowie die laufende Bereitstellung dieser Vorkehrungen nach Maßgaben der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3. Eine Entschädigung für im automatisierten Verfahren erteilte Auskünfte wird den Verpflichteten nicht gewährt.

§ 113 Manuelles Auskunftsverfahren

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, darf nach Maßgabe des Absatzes 2 die nach den §§ 95 und 111 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. Für die Auskunftserteilung nach Satz 3 sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) Die Auskunft darf nur erteilt werden, soweit eine in Absatz 3 genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 genannten Stellen unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt; an andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die in Absatz 3 genannten Stellen.

(3) Stellen im Sinne des Absatzes 1 sind

1. die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden;

2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden;

3. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst.

(4) Derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(5) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. Wer mehr als 100 000 Kunden hat, hat für die Entgegennahme der Auskunftsverlangen sowie für die Erteilung der zugehörigen Auskünfte eine gesicherte elektronische Schnittstelle nach Maßgabe der Technischen Richtlinie nach § 110 Absatz 3 bereitzuhalten, durch die auch die gegen die Kenntnisnahme der Daten durch Unbefugte gesicherte Übertragung gewährleistet ist. Dabei ist dafür Sorge zu tragen, dass jedes Auskunftsverlangen durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird.

§ 113a Verpflichtete; Entschädigung

(1) Die Verpflichtungen zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit nach den §§ 113b bis 113g beziehen sich auf Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer. Wer öffentlich zugängliche Tele-

kommunikationsdienste für Endnutzer erbringt, aber nicht alle der nach Maßgabe der §§ 113b bis 113g zu speichernden Daten selbst erzeugt oder verarbeitet, hat

1. sicherzustellen, dass die nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten oder verarbeiteten Daten gemäß § 113b Absatz 1 gespeichert werden, und
2. der Bundesnetzagentur auf deren Verlangen unverzüglich mitzuteilen, wer diese Daten speichert.

(2) Für notwendige Aufwendungen, die den Verpflichteten durch die Umsetzung der Vorgaben aus den §§ 113b, 113d bis 113g entstehen, ist eine angemessene Entschädigung zu zahlen, soweit dies zur Abwendung oder zum Ausgleich unbilliger Härten geboten erscheint. Für die Bemessung der Entschädigung sind die tatsächlich entstandenen Kosten maßgebend. Über Anträge auf Entschädigung entscheidet die Bundesnetzagentur.

§ 113b Pflichten zur Speicherung von Verkehrsdaten

(1) Die in § 113a Absatz 1 Genannten sind verpflichtet, Daten wie folgt im Inland zu speichern:

1. Daten nach den Absätzen 2 und 3 für zehn Wochen,
2. Standortdaten nach Absatz 4 für vier Wochen.

(2) Die Erbringer öffentlich zugänglicher Telefondienste speichern

1. die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2. Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone,
3. Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,
4. im Fall mobiler Telefondienste ferner
   a) die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,
   b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,
   c) Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,
5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.

Satz 1 gilt entsprechend

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

2. für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Erbringer öffentlich zugänglicher Telefondienste die in Satz 1 genannten Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert.

(3) Die Erbringer öffentlich zugänglicher Internetzugangsdienste speichern

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,

3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone.

(4) Im Fall der Nutzung mobiler Telefondienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. Bei öffentlich zugänglichen Internetzugangsdiensten ist im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Zusätzlich sind die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben.

(5) Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(6) Daten, die den in § 99 Absatz 2 genannten Verbindungen zugrunde liegen, dürfen auf Grund dieser Vorschrift nicht gespeichert werden. Dies gilt entsprechend für Telefonverbindungen, die von den in § 99 Absatz 2 genannten Stellen ausgehen. § 99 Absatz 2 Satz 2 bis 7 gilt entsprechend.

(7) Die Speicherung der Daten hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(8) Der nach § 113a Absatz 1 Verpflichtete hat die auf Grund des Absatzes 1 gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach Absatz 1, irreversibel zu löschen oder die irreversible Löschung sicherzustellen.

§ 113c Verwendung der Daten

(1) Die auf Grund des § 113b gespeicherten Daten dürfen

1. an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt;

2. an eine Gefahrenabwehrbehörde der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt;

3. durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 113 Absatz 1 Satz 3 verwendet werden.

(2) Für andere Zwecke als die in Absatz 1 genannten dürfen die auf Grund des § 113b gespeicherten Daten von den nach § 113a Absatz 1 Verpflichteten nicht verwendet werden.

(3) Die Übermittlung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 110 Absatz 2 und der Technischen Richtlinie nach § 110 Absatz 3. Die Daten sind so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b gespeichert waren. Nach Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

§ 113d Gewährleistung der Sicherheit der Daten

(1) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die auf Grund der Speicherpflicht nach § 113b Absatz 1 gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden.

(2) Die Maßnahmen umfassen insbesondere

1. den Einsatz eines besonders sicheren Verschlüsselungsverfahrens,

2. die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen,

3. die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet auf vom Internet entkoppelten Datenverarbeitungssystemen,

4. die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf Personen, die durch den Verpflichteten besonders ermächtigt sind, und

5. die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Verpflichteten besonders ermächtigt worden sind.

§ 113e Protokollierung

(1) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der auf Grund der Speicherpflicht nach § 113b Absatz 1 gespeicherten Daten protokolliert wird. Zu protokollieren sind

1. der Zeitpunkt des Zugriffs,
2. die auf die Daten zugreifenden Personen,
3. Zweck und Art des Zugriffs.

(2) Für andere Zwecke als die der Datenschutzkontrolle dürfen die Protokolldaten nicht verwendet werden.

(3) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die Protokolldaten nach einem Jahr gelöscht werden.

§ 113f Anforderungskatalog

(1) Bei der Umsetzung der Verpflichtungen gemäß den §§ 113b bis 113e ist ein besonders hoher Standard der Datensicherheit und Datenqualität zu gewährleisten. Die Einhaltung dieses Standards wird vermutet, wenn alle Anforderungen des Katalogs der technischen Vorkehrungen und sonstigen Maßnahmen erfüllt werden, den die Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt.

(2) Die Bundesnetzagentur überprüft fortlaufend die im Katalog nach Absatz 1 Satz 2 enthaltenen Anforderungen; hierbei berücksichtigt sie den Stand der Technik und der Fachdiskussion. Stellt die Bundesnetzagentur Änderungsbedarf fest, ist der Katalog im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unverzüglich anzupassen.

(3) § 109 Absatz 6 Satz 2 und 3 gilt entsprechend. § 109 Absatz 7 gilt mit der Maßgabe, dass an die Stelle der Anforderungen nach § 109 Absatz 1 bis 3 die Anforderungen nach Absatz 1 Satz 1, § 113b Absatz 7 und 8, § 113d und nach § 113e Absatz 1 und 3 treten.

§ 113g Sicherheitskonzept

Der nach § 113a Absatz 1 Verpflichtete hat in das Sicherheitskonzept nach § 109 Absatz 4 zusätzlich aufzunehmen,

1. welche Systeme zur Erfüllung der Verpflichtungen aus den §§ 113b bis 113e betrieben werden,
2. von welchen Gefährdungen für diese Systeme auszugehen ist und
3. welche technischen Vorkehrungen oder sonstigen Maßnahmen getroffen oder geplant sind, um diesen Gefährdungen entgegenzuwirken und die Verpflichtungen aus den §§ 113b bis 113e zu erfüllen.

Der nach § 113a Absatz 1 Verpflichtete hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach dem Beginn der Speicherung nach § 113b und unverzüglich bei jeder Änderung des Konzepts vorzulegen. Bleibt das Sicherheitskonzept unverändert, hat der nach § 113a Absatz 1 Verpflichtete dies gegenüber der Bundesnetzagentur im Abstand von jeweils zwei Jahren schriftlich zu erklären.

§ 114 Auskunftsersuchen des Bundesnachrichtendienstes

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt oder Übertragungswege betreibt, die für öffentlich zugängliche Telekommunikationsdienste genutzt werden, hat dem Bundesministerium für Wirtschaft und Technologie auf Anfrage entgeltfrei Auskünfte über die Strukturen der Telekommunikationsdienste und -netze sowie bevorstehende Änderungen zu erteilen. Einzelne Telekommunikationsvorgänge und Bestandsdaten von Teilnehmern dürfen nicht Gegenstand einer Auskunft nach dieser Vorschrift sein.

(2) Anfragen nach Absatz 1 sind nur zulässig, wenn ein entsprechendes Ersuchen des Bundesnachrichtendienstes vorliegt und soweit die Auskunft zur Erfüllung der Aufgaben nach den §§ 5 und 8 des Artikel 10-Gesetzes oder den §§ 6, 12 und 14 des BND-Gesetzes erforderlich ist. Die Verwendung einer nach dieser Vorschrift erlangten Auskunft zu anderen Zwecken ist ausgeschlossen.

§ 115 Kontrolle und Durchsetzung von Verpflichtungen

(1) Die Bundesnetzagentur kann Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Vorschriften des Teils 7 und der auf Grund dieses Teils ergangenen Rechtsverordnungen sowie der jeweils anzuwendenden Technischen Richtlinien sicherzustellen. Der Verpflichtete muss auf Anforderung der Bundesnetzagentur die hierzu erforderlichen Auskünfte erteilen. Die Bundesnetzagentur ist zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten zu betreten und zu besichtigen.

(2) Die Bundesnetzagentur kann nach Maßgabe des Verwaltungsvollstreckungsgesetzes Zwangsgelder wie folgt festsetzen:

1. bis zu 500 000 Euro zur Durchsetzung der Verpflichtungen nach § 108 Abs. 1, § 110 Abs. 1, 5 oder Abs. 6, einer Rechtsverordnung nach § 108 Absatz 3, einer Rechtsverordnung nach § 110 Abs. 2, einer Rechtsverordnung nach § 112 Abs. 3 Satz 1, der Technischen Richtlinie nach § 108 Absatz 4, der Technischen Richtlinie nach § 110 Abs. 3 oder der Technischen Richtlinie nach § 112 Abs. 3 Satz 3,

2. bis zu 100 000 Euro zur Durchsetzung der Verpflichtungen nach den §§ 109, 109a, 112 Absatz 1, 3 Satz 4, Absatz 5 Satz 1 und 2, § 113 Absatz 5 Satz 2 und 3 oder § 114 Absatz 1 und

3. bis zu 20 000 Euro zur Durchsetzung der Verpflichtungen nach § 111 Absatz 1, 4 und 5 oder § 113 Absatz 4 und 5 Satz 1.

Bei wiederholten Verstößen gegen § 111 Absatz 1 bis 5, § 112 Abs. 1, 3 Satz 4, Abs. 5 Satz 1 und 2 oder § 113 Absatz 4 und 5 Satz 1 kann die Tätigkeit des Verpflichteten durch Anordnung der Bundesnetzagentur dahin gehend eingeschränkt werden, dass der Kundenstamm bis zur Erfüllung der sich aus diesen Vorschriften ergebenden Verpflichtungen außer durch Vertragsablauf oder Kündigung nicht verändert werden darf.

(3) Darüber hinaus kann die Bundesnetzagentur bei Nichterfüllung von Verpflichtungen des Teils 7 den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen.

(4) Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden, tritt bei den Unternehmen an die Stelle der Kontrolle nach § 38 des Bundesdatenschutzgesetzes eine Kontrolle durch den Bundesbeauftragten für den Datenschutz entsprechend den §§ 21 und 24 bis 26 Abs. 1 bis 4 des Bundesdatenschutzgesetzes. Der Bundesbeauftragte für den Datenschutz richtet seine Beanstandungen an die Bundesnetzagentur und übermittelt dieser nach pflichtgemäßem Ermessen weitere Ergebnisse seiner Kontrolle.

(5) Das Fernmeldegeheimnis des Artikels 10 des Grundgesetzes wird eingeschränkt, soweit dies die Kontrollen nach Absatz 1 oder 4 erfordern.

Teil 10 Straf- und Bußgeldvorschriften

§ 148 Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. entgegen § 89 Satz 1 oder 2 eine Nachricht abhört oder in vergleichbarer Weise zur Kenntnis nimmt oder den Inhalt einer Nachricht oder die Tatsache ihres Empfangs einem anderen mitteilt oder

2. entgegen § 90 Abs. 1 Satz 1 eine dort genannte Sendeanlage oder eine sonstige Telekommunikationsanlage

   a) besitzt oder

   b) herstellt, vertreibt, einführt oder sonst in den Geltungsbereich dieses Gesetzes verbringt.

(2) Handelt der Täter in den Fällen des Absatzes 1 Nr. 2 Buchstabe b fahrlässig, so ist die Strafe Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.

§ 149 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4 eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zur Verfügung stellt,

2. entgegen § 6 Abs. 1 eine Meldung nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig macht,

3. entgegen § 17 Satz 2 eine Information weitergibt,

4. einer vollziehbaren Anordnung nach

   a) § 20 Absatz 1, 2 oder Absatz 3 Satz 1, § 23 Abs. 3 Satz 2, § 29 Abs. 1 Satz 1 Nr. 1 oder Abs. 2 Satz 1 oder 2, § 37 Abs. 3 Satz 2, auch in Verbindung mit § 38 Abs. 4 Satz 4, § 38 Abs. 4 Satz 2, auch in Verbindung mit § 39 Abs. 3 Satz 1 oder § 42 Abs. 4 Satz 1, auch in Verbindung mit § 18 Abs. 2 Satz 2,

   b) § 46 Absatz 9 Satz 1, § 67 Absatz 1 Satz 1, 2, 6 oder 7, § 77n Absatz 1 Satz 2, Absatz 4 Satz 2, Absatz 5 Satz 2 oder Absatz 6 Satz 2 oder § 109 Absatz 4 Satz 3 oder Satz 5,

   c) § 29 Abs. 1 Satz 2, § 39 Abs. 3 Satz 2, § 65 oder § 127 Absatz 2 Satz 1 Nummer 1, Satz 2 und 3

   zuwiderhandelt,

5. (weggefallen)

6. ohne Genehmigung nach § 30 Absatz 1 Satz 1, Absatz 2 Satz 2 zweiter Fall oder § 39 Abs. 1 Satz 1 ein Entgelt erhebt,

7. entgegen § 38 Abs. 1 Satz 1 oder 3 oder § 39 Abs. 3 Satz 4 ein Entgelt oder eine Entgeltmaßnahme nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zur Kenntnis gibt,

7a. einer Rechtsverordnung nach § 41a Absatz 1 oder einer vollziehbaren Anordnung auf Grund einer solchen Rechtsverordnung zuwiderhandelt, soweit die Rechtsverordnung für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist,

7b. entgegen § 41b Absatz 1 Satz 1 den Anschluss einer Telekommunikationsendeinrichtung verweigert,

7c. entgegen § 41b Absatz 1 Satz 3 die notwendigen Zugangsdaten und Informationen nicht, nicht richtig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig zur Verfügung stellt,

7d. entgegen § 41c Absatz 5 eine Leistung anbietet,

7e. entgegen § 43a Absatz 1 Satz 1 eine Information nicht, nicht richtig oder nicht vollständig zur Verfügung stellt,

7f. entgegen § 45k Absatz 1 Satz 1 eine Leistung ganz oder teilweise verweigert,

7g. einer Rechtsverordnung nach § 45n Absatz 1 oder einer vollziehbaren Anordnung auf Grund einer solchen Rechtsverordnung zuwiderhandelt, soweit die Rechtsverordnung für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist,

7h. entgegen § 45p Absatz 1 Satz 1, auch in Verbindung mit Satz 2, eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zur Verfügung stellt,

7i. entgegen § 45p Absatz 2 den Teilnehmer nicht, nicht richtig oder nicht vollständig unterrichtet,

7j. entgegen § 46 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, nicht sicherstellt, dass die Leistung beim Anbieterwechsel gegenüber dem Teilnehmer nicht unterbrochen wird,

7k. entgegen § 46 Absatz 1 Satz 2 den Telekommunikationsdienst unterbricht,

8. entgegen § 47 Abs. 1 Teilnehmerdaten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zur Verfügung stellt,

9. entgegen § 50 Abs. 3 Nr. 4 eine Anzeige nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet,

10. ohne Frequenzzuteilung nach § 55 Abs. 1 Satz 1 eine Frequenz nutzt,

11. ohne Übertragung nach § 56 Absatz 2 Satz 1 ein deutsches Orbit- oder Frequenznutzungsrecht ausübt,

12. einer vollziehbaren Auflage nach § 60 Abs. 2 Satz 1 zuwiderhandelt,

13. einer Rechtsverordnung nach § 66 Abs. 4 Satz 1 oder einer vollziehbaren Anordnung auf Grund einer solchen Rechtsverordnung zuwiderhandelt, soweit die Rechtsverordnung für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist,

13a. entgegen § 66a Satz 1, 2, 5, 6, 7 oder 8 eine Angabe nicht, nicht richtig oder nicht vollständig macht,

13b. entgegen § 66a Satz 3 die Preisangabe zeitlich kürzer anzeigt,

13c. entgegen § 66a Satz 4 einen Hinweis nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gibt,

13d. entgegen § 66b Abs. 1 Satz 1, auch in Verbindung mit Abs. 1 Satz 4 oder 5 oder Abs. 3 Satz 1, § 66b Abs. 1 Satz 3, auch in Verbindung mit Abs. 1 Satz 4 oder 5 oder § 66b Abs. 2 oder 3 Satz 2 einen dort genannten Preis nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig ansagt,

13e. entgegen § 66c Abs. 1 Satz 1, auch in Verbindung mit Satz 2, den dort genannten Preis nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig anzeigt,

13f. entgegen § 66d Abs. 1 oder 2 die dort genannte Preishöchstgrenze nicht einhält,

13g. entgegen § 66e Abs. 1 Satz 1, auch in Verbindung mit Satz 2, eine Verbindung nicht oder nicht rechtzeitig trennt,

13h. entgegen § 66f Abs. 1 Satz 1 einen Dialer einsetzt,

13i. entgegen § 66g Absatz 1 eine Warteschleife einsetzt,

13j. entgegen § 66g Absatz 2 nicht sicherstellt, dass der Anrufende informiert wird,

13k. entgegen § 66j Absatz 1 Satz 2 R-Gesprächsdienste anbietet,

13l. entgegen § 66k Absatz 1 Satz 1 nicht sicherstellt, dass eine vollständige Rufnummer übermittelt und gekennzeichnet wird,

13m. entgegen § 66k Absatz 1 Satz 3 eine Rufnummer oder eine Nummer für Kurzwahl-Sprachdienste übermittelt,

13n. entgegen § 66k Absatz 1 Satz 4 eine übermittelte Rufnummer verändert,

13o. entgegen § 66k Absatz 2 eine Rufnummer oder eine Nummer für Kurzwahl-Sprachdienste aufsetzt oder übermittelt,

14. entgegen § 87 Abs. 1 Satz 1 oder § 110 Abs. 1 Satz 2 oder 3 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

15. entgegen § 90 Abs. 3 für eine Sendeanlage oder eine sonstige Telekommunikationsanlage wirbt,

16. entgegen § 95 Abs. 2 oder § 96 Abs. 2 oder Abs. 3 Satz 1 Daten erhebt oder verwendet,

17. entgegen § 96 Abs. 1 Satz 3 oder § 97 Abs. 3 Satz 2 Daten nicht oder nicht rechtzeitig löscht,

17a. ohne Einwilligung nach § 98 Abs. 1 Satz 2 in Verbindung mit Satz 1 Daten verarbeitet,

17b. entgegen § 98 Absatz 1 Satz 2, auch in Verbindung mit Satz 5, eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gibt,

17c. entgegen § 100 Absatz 1 Satz 3 die Daten nicht oder nicht rechtzeitig löscht,

17d. entgegen § 100 Absatz 1 Satz 4 die Daten zu anderen Zwecken genutzt werden,

17e. entgegen § 102 Abs. 2 die Rufnummernanzeige unterdrückt oder veranlasst, dass diese unterdrückt wird,

18. entgegen § 106 Abs. 2 Satz 2 Daten oder Belege nicht oder nicht rechtzeitig löscht,

19. entgegen § 108 Absatz 1 Satz 1, auch in Verbindung mit Absatz 2, nicht sicherstellt, dass eine unentgeltliche Notrufverbindung möglich ist,

19a. entgegen § 108 Absatz 1 Satz 2, auch in Verbindung mit Absatz 2, oder einer Rechtsverordnung nach Absatz 3 Satz 1 Nummer 2, nicht sicherstellt, dass eine Notrufverbindung hergestellt wird,

20. entgegen § 108 Absatz 1 Satz 3, auch in Verbindung mit Absatz 2, oder einer Rechtsverordnung nach Absatz 3 Satz 1 Nummer 3, nicht sicherstellt, dass die Rufnummer des Anschlusses übermittelt wird, oder die dort genannten Daten übermittelt oder bereitgestellt werden,

21. entgegen § 109 Absatz 4 Satz 2 oder Satz 6 ein Sicherheitskonzept nicht oder nicht rechtzeitig vorlegt,

21a. entgegen § 109 Absatz 5 Satz 1 Nummer 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

21b. entgegen § 109a Absatz 1 Satz 1 oder Satz 2 die Bundesnetzagentur, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit oder einen Betroffenen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig benachrichtigt,

21c. entgegen § 109a Absatz 3 Satz 1 das dort genannte Verzeichnis nicht, nicht richtig oder nicht vollständig führt,

22. entgegen § 110 Abs. 1 Satz 1 Nr. 1 oder 1a in Verbindung mit einer Rechtsverordnung nach § 110 Abs. 2 Nr. 1 Buchstabe a eine technische Einrichtung nicht vorhält oder eine organisatorische Maßnahme nicht trifft,

23. entgegen § 110 Abs. 1 Satz 1 Nr. 2 Buchstabe b eine dort genannte Stelle nicht oder nicht rechtzeitig benennt,

24. entgegen § 110 Abs. 1 Satz 1 Nr. 3 einen Nachweis nicht oder nicht rechtzeitig erbringt,

25. entgegen § 110 Abs. 1 Satz 1 Nr. 4 eine Prüfung nicht gestattet,

26. entgegen § 110 Abs. 1 Satz 1 Nr. 5 die Aufstellung oder den Betrieb eines dort genannten Gerätes nicht duldet oder den Zugang zu einem solchen Gerät nicht gewährt,

27. entgegen § 110 Abs. 5 Satz 3 einen Mangel nicht oder nicht rechtzeitig beseitigt,

28. entgegen § 110 Abs. 6 Satz 1 einen Netzabschlusspunkt nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bereitstellt,

29. entgegen § 111 Absatz 1 Satz 1, auch in Verbindung mit Absatz 1 Satz 2 oder Absatz 2, oder entgegen § 111 Absatz 1 Satz 3 oder 5 oder Absatz 3 dort genannte Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erhebt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig speichert oder nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig berichtigt oder die Richtigkeit dort genannter Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig überprüft,

30. entgegen § 111 Absatz 4 Satz 2 eine Änderung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

30a. entgegen § 111 Absatz 5 Daten nicht oder nicht rechtzeitig löscht,

31. entgegen § 112 Abs. 1 Satz 5 nicht gewährleistet, dass die Bundesnetzagentur Daten aus den Kundendateien abrufen kann,

32. entgegen § 112 Abs. 1 Satz 6 nicht sicherstellt, dass ihm Abrufe nicht zur Kenntnis gelangen können,

33. entgegen § 113 Absatz 2 Satz 1 zweiter Halbsatz Daten nach § 113 Absatz 1 Satz 2 übermittelt,

34. entgegen § 113 Absatz 4 Satz 1 dort genannte Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

35. entgegen § 113 Absatz 4 Satz 2 Stillschweigen nicht wahrt,

36. entgegen § 113b Absatz 1, auch in Verbindung mit § 113b Absatz 7, Daten nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise, nicht für die vorgeschriebene Dauer oder nicht rechtzeitig speichert,

37. entgegen § 113b Absatz 1 in Verbindung mit § 113a Absatz 1 Satz 2 nicht sicherstellt, dass die dort genannten Daten gespeichert werden, oder eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

38. entgegen § 113b Absatz 8 Daten nicht oder nicht rechtzeitig löscht oder nicht sicherstellt, dass die Daten rechtzeitig gelöscht werden,

39. entgegen § 113c Absatz 2 Daten für andere als die genannten Zwecke verwendet,

40. entgegen § 113d Satz 1 nicht sicherstellt, dass Daten gegen unbefugte Kenntnisnahme und Verwendung geschützt werden,

41. entgegen § 113e Absatz 1 nicht sicherstellt, dass jeder Zugriff protokolliert wird,

42. entgegen § 113e Absatz 2 Protokolldaten für andere als die genannten Zwecke verwendet,

43. entgegen § 113e Absatz 3 nicht sicherstellt, dass Protokolldaten rechtzeitig gelöscht werden,

44. entgegen § 113g Satz 2 das Sicherheitskonzept nicht oder nicht rechtzeitig vorlegt oder

45. entgegen § 114 Abs. 1 Satz 1 oder § 127 Abs. 1 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt.

(1a) Ordnungswidrig handelt, wer gegen die Verordnung (EU) Nr. 531/2012 des Europäischen Parlaments und des Rates vom 13. Juni 2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union (ABl. L 172 vom 30.6.2012, S. 10), die zuletzt durch die Verordnung (EU) 2015/2120 (ABl. L 310 vom 26.11.2015, S. 1) geändert worden ist, verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 3 Absatz 5 Satz 2 einen Vertrag nicht oder nicht rechtzeitig vorlegt,

2. entgegen Artikel 5 Absatz 1 Satz 2 einem dort genannten Antrag nicht oder nicht unverzüglich nachkommt,

3. entgegen Artikel 6a ein dort genanntes Entgelt berechnet,

4. entgegen Artikel 6e Absatz 1 Unterabsatz 2 Satz 1 einen Aufschlag erhebt,

5. entgegen Artikel 6e Absatz 1 Unterabsatz 3 Satz 1 oder 3 ein Entgelt nicht richtig abrechnet,

6. entgegen Artikel 6e Absatz 1 Unterabsatz 3 Satz 2 eine andere Mindestabrechnungsdauer zugrunde legt,

7. entgegen Artikel 11 ein technisches Merkmal verändert,

8. entgegen Artikel 15 Absatz 2a Satz 1 in Verbindung mit Satz 2 eine Mitteilung nicht oder nicht rechtzeitig versendet,

9. entgegen Artikel 15 Absatz 3 Unterabsatz 6 Satz 1 nicht sicherstellt, dass eine dort genannte Meldung übermittelt wird,

10. entgegen Artikel 15 Absatz 3 Unterabsatz 7 Satz 3 die Erbringung oder Inrechnungstellung eines dort genannten Dienstes nicht oder nicht rechtzeitig einstellt,

11. entgegen Artikel 15 Absatz 3 Unterabsatz 8 eine dort genannte Änderung nicht oder nicht rechtzeitig vornimmt oder

12. entgegen Artikel 16 Absatz 4 Satz 2 eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt.

(1b) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union (ABl. L 310 vom 26.11.2015, S. 1) verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 3 Absatz 3 Unterabsatz 3 erster Halbsatz eine dort genannte Verkehrsmanagementmaßnahme anwendet,

2. entgegen Artikel 4 Absatz 1 Unterabsatz 1 Satz 1 nicht sicherstellt, dass ein dort genannter Vertrag die dort genannten Angaben enthält,

3. einer vollziehbaren Anordnung nach Artikel 5 Absatz 1 Unterabsatz 1 Satz 2 zuwiderhandelt oder

4. entgegen Artikel 5 Absatz 2 eine dort genannte Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt oder nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt.

(2) Die Ordnungswidrigkeit kann wie folgt geahndet werden:

1. in den Fällen des Absatzes 1 Nummer 4 Buchstabe a, Nummer 6, 10, 22, 27, 31 und 36 bis 40 und des Absatzes 1b Nummer 1 und 3 mit einer Geldbuße bis zu fünfhunderttausend Euro,

2. in den Fällen des Absatzes 1 Nummer 7a, 16 bis 17a, 18, 26, 29, 30a, 33 und 41 bis 43 mit einer Geldbuße bis zu dreihunderttausend Euro,

3. in den Fällen des Absatzes 1 Nummer 4 Buchstabe b, Nummer 7b bis 7d, 7g, 7h, 12 bis 13b, 13d bis 13o, 15, 17c, 19 bis 21, 21b, 30 und 44, des Absatzes 1a Nummer 1 bis 4 und des Absatzes 1b Nummer 2 mit einer Geldbuße bis zu hunderttausend Euro,

4. in den Fällen des Absatzes 1 Nummer 7, 8, 9, 11, 17b, 21a, 21c, 23 und 24 mit einer Geldbuße bis zu fünfzigtausend Euro und

5. in den übrigen Fällen der Absätze 1 bis 1b mit einer Geldbuße bis zu zehntausend Euro.

Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

(3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Bundesnetzagentur.

Anhang 2

Telemediengesetz

Zum 11. Januar 2018 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: Zuletzt geändert durch Art. 2 G v. 1.9.2016 | 3352

Hinweis: Änderung durch Art. 1 G v. 28.9.2017 | 3530 (Nr. 67) durch juris textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

Abschnitt 1 Allgemeine Bestimmungen

§ 1 Anwendungsbereich

(1) Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien). Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

(2) Dieses Gesetz gilt nicht für den Bereich der Besteuerung.

(3) Das Telekommunikationsgesetz und die Pressegesetze bleiben unberührt.

(4) Die an die Inhalte von Telemedien zu richtenden besonderen Anforderungen ergeben sich aus dem Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag).

(5) Dieses Gesetz trifft weder Regelungen im Bereich des internationalen Privatrechts noch regelt es die Zuständigkeit der Gerichte.

(6) Die besonderen Bestimmungen dieses Gesetzes für audiovisuelle Mediendienste auf Abruf gelten nicht für Dienste, die

1. ausschließlich zum Empfang in Drittländern bestimmt sind und
2. nicht unmittelbar oder mittelbar von der Allgemeinheit mit handelsüblichen Verbraucherendgeräten in einem Staat innerhalb des Geltungsbereichs der Richtlinie 89/552/EWG des Rates vom 3. Oktober 1989 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit (ABl. L 298 vom 17.10.1989, S. 23), die zuletzt durch die Richtlinie 2007/65/EG (ABl. L 332 vom 18.12.2007, S. 27) geändert worden ist, empfangen werden.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes

1. ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert,

2. ist niedergelassener Diensteanbieter jeder Anbieter, der mittels einer festen Einrichtung auf unbestimmte Zeit Telemedien geschäftsmäßig anbietet oder erbringt; der Standort der technischen Einrichtung allein begründet keine Niederlassung des Anbieters,

2a. ist drahtloses lokales Netzwerk ein Drahtloszugangssystem mit geringer Leistung und geringer Reichweite sowie mit geringem Störungsrisiko für weitere, von anderen Nutzern in unmittelbarer Nähe installierte Systeme dieser Art, welches nicht exklusive Grundfrequenzen nutzt,

3. ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen,

4. sind Verteildienste Telemedien, die im Wege einer Übertragung von Daten ohne individuelle Anforderung gleichzeitig für eine unbegrenzte Anzahl von Nutzern erbracht werden,

5. ist kommerzielle Kommunikation jede Form der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren, Dienstleistungen oder des Erscheinungsbilds eines Unternehmens, einer sonstigen Organisation oder einer natürlichen Person dient, die eine Tätigkeit im Handel, Gewerbe oder Handwerk oder einen freien Beruf ausübt; die Übermittlung der folgenden Angaben stellt als solche keine Form der kommerziellen Kommunikation dar:

   a) Angaben, die unmittelbaren Zugang zur Tätigkeit des Unternehmens oder der Organisation oder Person ermöglichen, wie insbesondere ein Domain-Name oder eine Adresse der elektronischen Post,

   b) Angaben in Bezug auf Waren und Dienstleistungen oder das Erscheinungsbild eines Unternehmens, einer Organisation oder Person, die unabhängig und insbesondere ohne finanzielle Gegenleistung gemacht werden.

6. sind „audiovisuelle Mediendienste auf Abruf“ Telemedien mit Inhalten, die nach Form und Inhalt fernsehähnlich sind und die von einem Diensteanbieter zum individuellen Abruf zu einem vom Nutzer gewählten Zeitpunkt und aus einem vom Diensteanbieter festgelegten Inhaltekatalog bereitgestellt werden.

Einer juristischen Person steht eine Personengesellschaft gleich, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben und Verbindlichkeiten einzugehen.

§ 2a Europäisches Sitzland

(1) Innerhalb des Geltungsbereichs der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. L 178 vom 17.7.2000, S. 1) bestimmt sich das Sitzland des Diensteanbieters danach, wo dieser seine Geschäftstätigkeit tatsächlich ausübt. Dies ist der Ort, an dem sich der Mittelpunkt der Tätigkeiten des Diensteanbieters im Hinblick auf ein bestimmtes Telemedienangebot befindet.

(2) Abweichend von Absatz 1 gilt innerhalb des Geltungsbereichs der Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) (ABl. L 95 vom 15.4.2010, S. 1) bei audiovisuellen Mediendiensten auf Abruf Deutschland als Sitzland des Diensteanbieters, wenn

1. die Hauptverwaltung in Deutschland liegt und die redaktionellen Entscheidungen über den audiovisuellen Mediendienst dort getroffen werden,

2. die Hauptverwaltung in Deutschland liegt und die redaktionellen Entscheidungen über den audiovisuellen Mediendienst in einem anderen Mitgliedstaat der Europäischen Union getroffen werden, jedoch

   a) ein wesentlicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals in Deutschland tätig ist,

   b) ein wesentlicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals sowohl in Deutschland als auch in dem anderen Mitgliedstaat tätig ist oder

   c) ein wesentlicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals weder in Deutschland noch in dem anderen Mitgliedstaat tätig ist, aber der Diensteanbieter zuerst in Deutschland seine Tätigkeit aufgenommen hat und eine dauerhafte und tatsächliche Verbindung mit der Wirtschaft Deutschlands fortbesteht, oder

3. die Hauptverwaltung in Deutschland liegt und die redaktionellen Entscheidungen über den audiovisuellen Mediendienst in einem Drittstaat getroffen werden oder umgekehrt, aber ein wesentlicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals in Deutschland tätig ist.

(3) Für audiovisuelle Mediendiensteanbieter, die nicht bereits aufgrund ihrer Niederlassung der Rechtshoheit Deutschlands oder eines anderen Mitgliedstaats der Europäischen Union unterliegen, gilt Deutschland als Sitzland, wenn sie

1. eine in Deutschland gelegene Satelliten-Bodenstation für die Aufwärtsstrecke nutzen oder

2. zwar keine in einem Mitgliedstaat der Europäischen Union gelegene Satelliten-Bodenstation für die Aufwärtsstrecke nutzen, aber eine Deutschland zugewiesene Übertragungskapazität eines Satelliten nutzen.

Liegt keines dieser beiden Kriterien vor, gilt Deutschland auch als Sitzland für Diensteanbieter, die in Deutschland gemäß den Artikeln 49 bis 55 des Vertrages über die Arbeitsweise der Europäischen Union niedergelassen sind.

§ 2a dient der Umsetzung der Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) (ABl. L 95 vom 15.4.2010, S. 1).

§ 3 Herkunftslandprinzip

(1) In der Bundesrepublik Deutschland nach § 2a niedergelassene Diensteanbieter und ihre Telemedien unterliegen den Anforderungen des deutschen Rechts auch dann, wenn die Telemedien in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 89/552/EWG geschäftsmäßig angeboten oder erbracht werden.

(2) Der freie Dienstleistungsverkehr von Telemedien, die in der Bundesrepublik Deutschland von Diensteanbietern geschäftsmäßig angeboten oder erbracht werden, die in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 89/552/EWG niedergelassen sind, wird nicht eingeschränkt. Absatz 5 bleibt unberührt.

(3) Von den Absätzen 1 und 2 bleiben unberührt

1. die Freiheit der Rechtswahl,

2. die Vorschriften für vertragliche Schuldverhältnisse in Bezug auf Verbraucherverträge,

3. gesetzliche Vorschriften über die Form des Erwerbs von Grundstücken und grundstücksgleichen Rechten sowie der Begründung, Übertragung, Änderung oder Aufhebung von dinglichen Rechten an Grundstücken und grundstücksgleichen Rechten,

4. das für den Schutz personenbezogener Daten geltende Recht.

(4) Die Absätze 1 und 2 gelten nicht für

1. die Tätigkeit von Notaren sowie von Angehörigen anderer Berufe, soweit diese ebenfalls hoheitlich tätig sind,

2. die Vertretung von Mandanten und die Wahrnehmung ihrer Interessen vor Gericht,

3. die Zulässigkeit nicht angeforderter kommerzieller Kommunikationen durch elektronische Post,

4. Gewinnspiele mit einem einen Geldwert darstellenden Einsatz bei Glücksspielen, einschließlich Lotterien und Wetten,

5. die Anforderungen an Verteildienste,

6. das Urheberrecht, verwandte Schutzrechte, Rechte im Sinne der Richtlinie 87/54/EWG des Rates vom 16. Dezember 1986 über den Rechtsschutz der Topographien von Halbleitererzeugnissen (ABl. EG Nr. L 24 S. 36) und der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken (ABl. EG Nr. L 77 S. 20) sowie für gewerbliche Schutzrechte,

7. die Ausgabe elektronischen Geldes durch Institute, die gemäß Artikel 8 Abs. 1 der Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (ABl. EG Nr. L 275 S. 39) von der Anwendung einiger oder aller Vorschriften dieser Richtlinie und von der Anwendung der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates vom 20. März 2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (ABl. EG Nr. L 126 S. 1) freigestellt sind,

8. Vereinbarungen oder Verhaltensweisen, die dem Kartellrecht unterliegen,

9. die von den §§ 12, 13a bis 13c, 55a, 83, 110a bis 110d, 111b und 111c des Versicherungsaufsichtsgesetzes in der Fassung der Bekanntmachung vom 17. Dezember 1992 (BGBl. 1993 | S. 2), das zuletzt durch Artikel 2 des Gesetzes vom 29. Juli 2009 (BGBl. | S. 2305) geändert worden ist, in der am 31. Dezember 2015 geltenden Fassung und der Versicherungsberichterstattungs-Verordnung erfassten Bereiche, die Regelungen über das auf Versicherungsverträge anwendbare Recht sowie für Pflichtversicherungen.

(5) Das Angebot und die Erbringung von Telemedien durch einen Diensteanbieter, der in einem anderen Staat im Geltungsbereich der Richtlinien 2000/31/EG oder 89/552/EWG niedergelassen ist, unterliegen abweichend von Absatz 2 den Einschränkungen des innerstaatlichen Rechts, soweit dieses dem Schutz

1. der öffentlichen Sicherheit und Ordnung, insbesondere im Hinblick auf die Verhütung, Ermittlung, Aufklärung, Verfolgung und Vollstreckung von Straftaten und Ordnungswidrigkeiten, einschließlich des Jugendschutzes und der Bekämpfung der Hetze aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität sowie von Verletzungen der Menschenwürde einzelner Personen sowie die Wahrung nationaler Sicherheits- und Verteidigungsinteressen,

2. der öffentlichen Gesundheit,

3. der Interessen der Verbraucher, einschließlich des Schutzes von Anlegern,

vor Beeinträchtigungen oder ernsthaften und schwerwiegenden Gefahren dient und die auf der Grundlage des innerstaatlichen Rechts in Betracht kommenden Maßnahmen in einem angemessenen Verhältnis zu diesen Schutzzielen stehen. Für das Verfahren zur Einleitung von Maßnahmen nach Satz 1 – mit Ausnahme von gerichtlichen Verfahren einschließlich etwaiger Vorverfahren und der Verfolgung von Straftaten einschließlich der Strafvollstreckung und von Ordnungswidrigkeiten – sehen Artikel 3 Abs. 4 und 5 der Richtlinie 2000/31/EG sowie Artikel 2a Absatz 4 und 5 der Richtlinie 89/552/EWG Konsultations- und Informationspflichten vor.

Abschnitt 2 Zulassungsfreiheit und Informationspflichten

§ 4 Zulassungsfreiheit

Telemedien sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

§ 5 Allgemeine Informationspflichten

(1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen,

2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,

3. soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,

4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,

5. soweit der Dienst in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens dreijährige Berufsausbildung abschließen (ABl. EG Nr. L 19 S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung

beruflicher Befähigungsnachweise in Ergänzung zur Richtlinie 89/48/EWG (ABl. EG Nr. L 209 S. 25, 1995 Nr. L 17 S. 20), zuletzt geändert durch die Richtlinie 97/38/EG der Kommission vom 20. Juni 1997 (ABl. EG Nr. L 184 S. 31), angeboten oder erbracht wird, Angaben über

a) die Kammer, welcher die Diensteanbieter angehören,

b) die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,

c) die Bezeichnung der berufsrechtlichen Regelungen und dazu, wie diese zugänglich sind,

6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung besitzen, die Angabe dieser Nummer,

7. bei Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung, die sich in Abwicklung oder Liquidation befinden, die Angabe hierüber.

(2) Weitergehende Informationspflichten nach anderen Rechtsvorschriften bleiben unberührt.

§ 6 Besondere Informationspflichten bei kommerziellen Kommunikationen

(1) Diensteanbieter haben bei kommerziellen Kommunikationen, die Telemedien oder Bestandteile von Telemedien sind, mindestens die folgenden Voraussetzungen zu beachten:

1. Kommerzielle Kommunikationen müssen klar als solche zu erkennen sein.

2. Die natürliche oder juristische Person, in deren Auftrag kommerzielle Kommunikationen erfolgen, muss klar identifizierbar sein.

3. Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke müssen klar als solche erkennbar sein, und die Bedingungen für ihre Inanspruchnahme müssen leicht zugänglich sein sowie klar und unzweideutig angegeben werden.

4. Preisausschreiben oder Gewinnspiele mit Werbecharakter müssen klar als solche erkennbar und die Teilnahmebedingungen leicht zugänglich sein sowie klar und unzweideutig angegeben werden.

(2) Werden kommerzielle Kommunikationen per elektronischer Post versandt, darf in der Kopf- und Betreffzeile weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.

(3) Die Vorschriften des Gesetzes gegen den unlauteren Wettbewerb bleiben unberührt.

Abschnitt 3 Verantwortlichkeit

§ 7 Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

(3) Verpflichtungen zur Entfernung von Informationen oder zur Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen aufgrund von gerichtlichen oder behördlichen Anordnungen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren.

(4) Wurde ein Telemediendienst von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen und besteht für den Inhaber dieses Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuhelfen, so kann der Inhaber des Rechts von dem betroffenen Diensteanbieter nach § 8 Absatz 3 die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein. *3*Ein Anspruch gegen den Diensteanbieter auf Erstattung der vor- und außergerichtlichen Kosten für die Geltendmachung und Durchsetzung des Anspruchs nach Satz 1 besteht außer in den Fällen des § 8 Absatz 1 Satz 3 nicht.

§ 8 Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Sofern diese Diensteanbieter nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Die Sätze 1 und 2 finden keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

(3) Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

(4) Diensteanbieter nach § 8 Absatz 3 dürfen von einer Behörde nicht verpflichtet werden,

1. vor Gewährung des Zugangs

   a) die persönlichen Daten von Nutzern zu erheben und zu speichern (Registrierung) oder

   b) die Eingabe eines Passworts zu verlangen oder

2. das Anbieten des Dienstes dauerhaft einzustellen.

Davon unberührt bleibt, wenn ein Diensteanbieter auf freiwilliger Basis die Nutzer identifiziert, eine Passworteingabe verlangt oder andere freiwillige Maßnahmen ergreift.

§ 9 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen

Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie

1. die Informationen nicht verändern,

2. die Bedingungen für den Zugang zu den Informationen beachten,

3. die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,

4. die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und

5. unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

   § 8 Abs. 1 Satz 2 gilt entsprechend.

§ 10 Speicherung von Informationen

Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern

1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.

Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Abschnitt 4 Datenschutz

§ 11 Anbieter-Nutzer-Verhältnis

(1) Die Vorschriften dieses Abschnitts gelten nicht für die Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien, soweit die Bereitstellung solcher Dienste

1. im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder
2. innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

(2) Nutzer im Sinne dieses Abschnitts ist jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

(3) Bei Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, gelten für die Erhebung und Verwendung personenbezogener Daten der Nutzer nur § 15 Absatz 8 und § 16 Absatz 2 Nummer 4.

§ 12 Grundsätze

(1) Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

(3) Soweit nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht automatisiert verarbeitet werden.

§ 13 Pflichten des Diensteanbieters

(1) Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs 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. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. *2*Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

(2) Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

(3) Der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Recht nach Absatz 2 Nr. 4 hinzuweisen. Absatz 1 Satz 3 gilt entsprechend.

(4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 2 gesperrt werden,
3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,

5. Daten nach § 15 Abs. 2 nur für Abrechnungszwecke zusammengeführt werden können und

6. Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

An die Stelle der Löschung nach Satz 1 Nr. 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

(5) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(6) Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

(7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und

2. diese

a) gegen Verletzungen des Schutzes personenbezogener Daten und

b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

(8) Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.

§ 14 Bestandsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten).

(2) Auf Anordnung der zuständigen Stellen darf der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahren-

abwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

(3) Der Diensteanbieter darf darüber hinaus im Einzelfall Auskunft über bei ihm vorhandene Bestandsdaten erteilen, soweit dies zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger Inhalte, die von § 1 Absatz 3 des Netzwerkdurchsetzungsgesetzes erfasst werden, erforderlich ist.

(4) Für die Erteilung der Auskunft nach Absatz 3 ist eine vorherige gerichtliche Anordnung über die Zulässigkeit der Auskunftserteilung erforderlich, die vom Verletzten zu beantragen ist. Für den Erlass dieser Anordnung ist das Landgericht ohne Rücksicht auf den Streitwert zuständig. Örtlich zuständig ist das Gericht, in dessen Bezirk der Verletzte seinen Wohnsitz, seinen Sitz oder eine Niederlassung hat. Die Entscheidung trifft die Zivilkammer. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die Kosten der richterlichen Anordnung trägt der Verletzte. Gegen die Entscheidung des Landgerichts ist die Beschwerde statthaft.

(5) Der Diensteanbieter ist als Beteiligter zu dem Verfahren nach Absatz 4 hinzuzuziehen. Er darf den Nutzer über die Einleitung des Verfahrens unterrichten.

§ 15 Nutzungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. Merkmale zur Identifikation des Nutzers,
2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

(2) Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemedien zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.

(3) Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer

auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren.

(5) Der Diensteanbieter darf an andere Diensteanbieter oder Dritte Abrechnungsdaten übermitteln, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer erforderlich ist. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen anonymisierte Nutzungsdaten übermittelt werden. § 14 Absatz 2 bis 5 findet entsprechende Anwendung.

(6) Die Abrechnung über die Inanspruchnahme von Telemedien darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Telemedien nicht erkennen lassen, es sei denn, der Nutzer verlangt einen Einzelnachweis.

(7) Der Diensteanbieter darf Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers verarbeitet werden, höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung speichern. Werden gegen die Entgeltforderung innerhalb dieser Frist Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen, dürfen die Abrechnungsdaten weiter gespeichert werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen ist.

(8) Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus nur verwenden, soweit dies für Zwecke der Rechtsverfolgung erforderlich ist. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.

§ 15a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.

Abschnitt 5 Bußgeldvorschriften

§ 16 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer absichtlich entgegen § 6 Abs. 2 Satz 1 den Absender oder den kommerziellen Charakter der Nachricht verschleiert oder verheimlicht.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 5 Abs. 1 eine Information nicht, nicht richtig oder nicht vollständig verfügbar hält,

2. entgegen § 13 Abs. 1 Satz 1 oder 2 den Nutzer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

3. einer Vorschrift des § 13 Abs. 4 Satz 1 Nr. 1 bis 4 oder 5 oder Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a über eine dort genannte Pflicht zur Sicherstellung zuwiderhandelt,

4. entgegen § 14 Abs. 1 oder § 15 Abs. 1 Satz 1 oder Abs. 8 Satz 1 oder 2 personenbezogene Daten erhebt oder verwendet oder nicht oder nicht rechtzeitig löscht oder

5. entgegen § 15 Abs. 3 Satz 3 ein Nutzungsprofil mit Daten über den Träger des Pseudonyms zusammenführt.

(3) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

Anhang 3

Bundesdatenschutzgesetz

Zum 11. Januar 2018 aktuellste verfügbare Fassung der Gesamtausgabe; Gesamtausgabe in der Gültigkeit bis 24. Mai 2018.

Stand: Neugefasst durch Bekanntmachung vom 13. Januar 2003 | 66; zuletzt geändert durch Art. 10 Abs. 2 G v. 31. Oktober 2017 | 3618

Hinweis: Gesetz aufgehoben durch Art. 8 Abs. 1 Satz 2 G v. 30. Juni 2017 | 2097 mWv 25. Mai 2018; ersetzt durch G 204-4 v. 30. Juni 2017 | 2097 (BDSG 2018)

Erster Abschnitt

Allgemeine und gemeinsame Bestimmungen

Fünfter Abschnitt

Schlussvorschriften

Sechster Abschnitt

Übergangsvorschriften

Erster Abschnitt Allgemeine und gemeinsame Bestimmungen

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,

2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie

a) Bundesrecht ausführen oder

b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

§ 2 Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder

2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

   Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,

2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

   a) die Daten an den Dritten weitergegeben werden oder

   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,

2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

(11) Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer,

2. zu ihrer Berufsbildung Beschäftigte,

3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),

4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,

5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,

6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,

8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

§ 3a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

   und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,

2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder

3. der Organe und Einrichtungen der Europäischen Gemeinschaften

gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30a nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten

erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

(2) Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend. Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.

§ 4c Ausnahmen

(1) Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern

1. der Betroffene seine Einwilligung gegeben hat,

2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,

3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,

4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,

5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder

6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.

(2) Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Bei den Post- und Telekommunikationsunternehmen ist die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.

(3) Die Länder teilen dem Bund die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.

§ 4d Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Per-

sonen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung,
2. zum Zweck der anonymisierten Übermittlung oder
3. für Zwecke der Markt- oder Meinungsforschung

gespeichert werden.

(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

§ 4e Inhalt der Meldepflicht

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,

2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,

3. Anschrift der verantwortlichen Stelle,

4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,

5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,

7. Regelfristen für die Löschung der Daten,

8. eine geplante Datenübermittlung in Drittstaaten,

9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

§ 4f Beauftragter für den Datenschutz

(1) Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für die nichtöffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung

der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden. Ist nach Absatz 1 ein Beauftragter für den Datenschutz zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(4a) Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nichtöffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(5) Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Er-

füllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

§ 4g Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Der Beauftragte für den Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.

(2a) Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.

(3) Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde.

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das

Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6 Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

(3) Personenbezogene Daten über die Ausübung eines Rechts des Betroffenen, das sich aus diesem Gesetz oder aus einer anderen Vorschrift über den Datenschutz ergibt, dürfen nur zur Erfüllung der sich aus der Ausübung des Rechts ergebenden Pflichten der verantwortlichen Stelle verwendet werden.

§ 6a Automatisierte Einzelentscheidung

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder

2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert.

(3) Das Recht des Betroffenen auf Auskunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

§ 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei der Videoüberwachung von

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder
2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Absatz 1 Satz 2 gilt entsprechend. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 7 Schadensersatz

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten

einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130.000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130.000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt § 254 des Bürgerlichen Gesetzbuchs.

(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 9a Datenschutzaudit

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

§ 10 Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn das für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesministerium zugestimmt hat.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann.

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,

   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

   die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Zweiter Abschnitt Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt Rechtsgrundlagen der Datenverarbeitung

§ 12 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 16, 19 bis 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder

2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.

(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28 Absatz 2 Nummer 2 und die §§ 32 bis 35 anstelle der §§ 13 bis 16 und 19 bis 20.

§ 13 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,
2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,
8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder
9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§ 14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben er-

forderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder

2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

   Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 15 Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und

2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 10 Abs. 4 bleibt unberührt.

(3) Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, dass eine Tren-

nung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 16 Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder

2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 17

(weggefallen)

§ 18 Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das Gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre automatisierten Verarbeitungen haben sie die Angaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

Zweiter Unterabschnitt Rechte des Betroffenen

§ 19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften

nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,

2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§ 19a Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger

oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder

3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.

(3) § 19 Abs. 2 bis 4 gilt entsprechend.

§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder

2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die Behörde im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(9) (weggefallen)

§ 21 Anrufung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Jedermann kann sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Dritter Unterabschnitt Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

§ 22 Wahl und Unabhängigkeit der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Deutsche Bundestag wählt ohne Aussprache auf Vorschlag der Bundesregierung die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Die oder der Bundesbeauftragte muss bei ihrer oder seiner Wahl das 35. Lebensjahr vollendet haben. Die oder der Gewählte ist von der Bundespräsidentin oder dem Bundespräsidenten zu ernennen.

(2) Die oder der Bundesbeauftragte leistet vor der Bundespräsidentin oder dem Bundespräsidenten folgenden Eid:

„Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe."

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit der oder des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Die oder der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Sie oder er ist in Ausübung ihres oder seines Amtes unabhängig und nur dem Gesetz unterworfen.

(5) Die oder der Bundesbeauftragte ist eine oberste Bundesbehörde. Der Dienstsitz ist Bonn. Die Beamtinnen und Beamten der oder des Bundesbeauftragten sind Beamtinnen und Beamte des Bundes.

(5a) Die oder der Bundesbeauftragte kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Bundes übertragen, soweit hierdurch die Unabhängigkeit der oder des Bundesbeauftragten nicht beeinträchtigt wird. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

(6) Die Leitende Beamtin oder der Leitende Beamte nimmt die Rechte der oder des Bundesbeauftragten wahr, wenn die oder der Bundesbeauftragte an der Ausübung ihres oder seines Amtes verhindert ist oder wenn ihr oder sein Amtsverhältnis endet und sie oder er nicht zur Weiterführung der Geschäfte verpflichtet ist. Absatz 4 Satz 2 ist entsprechend anzuwenden.

§ 23 Rechtsstellung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Das Amtsverhältnis der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,
2. mit der Entlassung.

Die Bundespräsidentin oder der Bundespräsident entlässt die Bundesbeauftragte oder den Bundesbeauftragten, wenn diese oder dieser es verlangt oder auf Vorschlag der Präsidentin oder des Präsidenten des Bundestages, wenn Gründe vorliegen, die bei einer Richterin auf Lebenszeit oder einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält die oder der Bundesbeauftragte eine von der Bundespräsidentin oder dem Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Endet das Amtsverhältnis mit Ablauf der Amtszeit, ist die oder der Bundesbeauftragte verpflichtet, auf Ersuchen der Präsidentin oder des Präsidenten des Bundestages die Geschäfte bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers weiterzuführen.

(2) Die oder der Bundesbeauftragte darf neben ihrem oder seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Sie oder er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Die oder der Bundesbeauftragte hat der Präsidentin oder dem Präsidenten des Bundestages Mitteilung über Geschenke zu machen, die sie oder er in Bezug auf das Amt erhält. Die Präsidentin oder der Präsident des Bundestages entscheidet über die Verwendung der Geschenke. Sie oder er kann Verfahrensvorschriften erlassen.

(4) Die oder der Bundesbeauftragte ist berechtigt, über Personen, die ihr oder ihm in ihrer oder seiner Eigenschaft als Bundesbeauftragte oder Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiterinnen und Mitarbeiter der oder des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts die oder der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht der oder des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihr oder ihm nicht gefordert werden.

(5) Die oder der Bundesbeauftragte ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekanntgewordenen Angelegenheiten

Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die oder der Bundesbeauftragte entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie oder er über solche Angelegenheiten vor Gericht oder außergerichtlich aussagt oder Erklärungen abgibt; wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Bundesbeauftragten erforderlich. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. Für die Bundesbeauftragte oder den Bundesbeauftragten und ihre oder seine Mitarbeiterinnen und Mitarbeiter gelten die §§ 93, 97, 105 Abs. 1, § 111 Abs. 5 in Verbindung mit § 105 Abs. 1 sowie § 116 Abs. 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben der oder des Auskunftspflichtigen oder der für sie oder ihn tätigen Personen handelt. Stellt die oder der Bundesbeauftragte einen Datenschutzverstoß fest, ist sie oder er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.

(6) Die oder der Bundesbeauftragte darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde

1. dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit der Bundesrepublik Deutschland oder ihre Beziehungen zu anderen Staaten, oder

2. Grundrechte verletzen.

Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Bundesregierung zuzurechnen sind oder sein könnten, darf die oder der Bundesbeauftragte nur im Benehmen mit der Bundesregierung aussagen. § 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.

(7) Die oder der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der Besoldungsgruppe B 11 sowie den Familienzuschlag entsprechend Anlage V des Bundesbesoldungsgesetzes. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im Übrigen sind § 12 Abs 6 sowie die §§ 13 bis 20 und 21a Abs. 5 des Bundesministergesetzes mit den Maßgaben anzuwenden, dass an die Stelle der vierjährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 und 21a Abs. 5 des Bundesministergesetzes berechnet sich das Ruhegehalt der oder des

Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und die oder der Bundesbeauftragte sich unmittelbar vor ihrer oder seiner Wahl zur oder zum Bundesbeauftragten als Beamtin oder Beamter oder als Richterin oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 11 zu durchlaufenden Amt befunden hat.

(8) Absatz 5 Satz 5 bis 7 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 24 Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) Die Kontrolle der oder des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs, und

2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegen, unterliegen nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten, es sei denn, die Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber der oder dem Bundesbeauftragten widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle der oder des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, die Bundesbeauftragte oder den Bundesbeauftragten und ihre oder seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur der oder dem Bundesbeauftragten selbst und den von ihr oder ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Die oder der Bundesbeauftragte teilt das Ergebnis ihrer oder seiner Kontrolle der öffentlichen Stelle mit. Damit kann sie oder er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25 Beanstandungen durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Stellt die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,

2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,

3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,

4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet die oder der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Die oder der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an die Bundesbeauftragte oder den Bundesbeauftragten zu.

§ 26 Weitere Aufgaben der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Sie oder er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat die oder der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht die oder der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Die oder der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Die oder der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch die Bundesbeauftragte oder den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Die oder der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. § 38 Abs. 1 Satz 4 und 5 gilt entsprechend.

Dritter Abschnitt Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt Rechtsgrundlagen der Datenverarbeitung

§ 27 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch

1. nicht-öffentliche Stellen,

2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,

   b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

   Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Aus-

schluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,

2. soweit es erforderlich ist,

   a) zur Wahrung berechtigter Interessen eines Dritten oder

   b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

   und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,

2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder

3. für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

(3b) Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch

keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 4 des Strafgesetzbuchs genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. 4Absatz 2 Nummer 2 Buchstabe b gilt entsprechend.

§ 28a Datenübermittlung an Auskunfteien

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,

3. der Betroffene die Forderung ausdrücklich anerkannt hat,

4. a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

d) der Betroffene die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

(2) Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

§ 28b Scoring

Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,

2. im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,

3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,

4. im Fall der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder

3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und

2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Absatz 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Satz 1 Nr. 1 sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden. Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. *2*Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

(6) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(7) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 6 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 6a bleibt unberührt.

§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) § 29 gilt nicht.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

§ 30a Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung

(1) Das geschäftsmäßige Erheben, Verarbeiten oder Nutzen personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung gegenüber dem Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt.

Besondere Arten personenbezogener Daten (§ 3 Absatz 9) dürfen nur für ein bestimmtes Forschungsvorhaben erhoben, verarbeitet oder genutzt werden.

(2) Für Zwecke der Markt- oder Meinungsforschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet oder genutzt werden. Daten, die nicht aus allgemein zugänglichen Quellen entnommen worden sind und die die verantwortliche Stelle auch nicht veröffentlichen darf, dürfen nur für das Forschungsvorhaben verarbeitet oder genutzt werden, für das sie erhoben worden sind. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, wenn sie zuvor so anonymisiert werden, dass ein Personenbezug nicht mehr hergestellt werden kann.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Zweck des Forschungsvorhabens, für das die Daten erhoben worden sind, möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies nach dem Zweck des Forschungsvorhabens erforderlich ist.

(4) § 29 gilt nicht.

(5) § 28 Absatz 4 und 6 bis 9 gilt entsprechend.

§ 31 Besondere Zweckbindung

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

Zweiter Unterabschnitt Rechte des Betroffenen

§ 33 Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder aus-

schließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,

4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,

5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

7. die Daten für eigene Zwecke gespeichert sind und

   a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder

   b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,

8. die Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert sind und

   a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder

   b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Absatz 2 Satz 2)

und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist,

9. aus allgemein zugänglichen Quellen entnommene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung gespeichert sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

§ 34 Auskunft an den Betroffenen

(1) Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(1a) Im Fall des § 28 Absatz 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. Satz 1 gilt entsprechend für den Empfänger.

(2) Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,

2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und

3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle

1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

Hat eine andere als die für die Entscheidung verantwortliche Stelle

1. den Wahrscheinlichkeitswert oder

2. einen Bestandteil des Wahrscheinlichkeitswerts

berechnet, hat sie die insoweit zur Erfüllung der Auskunftsansprüche nach den Sätzen 1 und 2 erforderlichen Angaben auf Verlangen der für die Entscheidung verantwortlichen Stelle an diese zu übermitteln. Im Fall des Satzes 3 Nr. 1 hat die für die Entscheidung verantwortliche Stelle den Betroffenen zur Geltendmachung seiner Auskunftsansprüche unter Angabe des Namens und der Anschrift der anderen Stelle sowie der zur Bezeichnung des Einzelfalls

notwendigen Angaben unverzüglich an diese zu verweisen, soweit sie die Auskunft nicht selbst erteilt. In diesem Fall hat die andere Stelle, die den Wahrscheinlichkeitswert berechnet hat, die Auskunftsansprüche nach den Sätzen 1 und 2 gegenüber dem Betroffenen unentgeltlich zu erfüllen. Die Pflicht der für die Berechnung des Wahrscheinlichkeitswerts verantwortlichen Stelle nach Satz 3 entfällt, soweit die für die Entscheidung verantwortliche Stelle von ihrem Recht nach Satz 4 Gebrauch macht.

(3) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die

1. gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,

2. die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung nutzt.

Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(4) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,

2. die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,

3. die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie

4. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

(5) Die nach den Absätzen 1a bis 4 zum Zweck der Auskunftserteilung an den Betroffenen gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verwendet werden; für andere Zwecke sind sie zu sperren.

(6) Die Auskunft ist auf Verlangen in Textform zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(7) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(8) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen. Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann nicht verlangt werden, wenn

1. besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder

2. die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 zu berichtigen oder nach § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(9) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten zu verschaffen. Er ist hierauf hinzuweisen.

§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,

2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,

3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder

4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Fall des Absatzes 2 Satz 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(4a) Die Tatsache der Sperrung darf nicht übermittelt werden.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zweck der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Dritter Unterabschnitt Aufsichtsbehörde

§§ 36 und 37 (weggefallen)

§ 38 Aufsichtsbehörde

(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 gilt entsprechend. Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. § 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.

(2) Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.

(3) Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. *4*Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

§ 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Vierter Abschnitt Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,

2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,

3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§ 42 Datenschutzbeauftragter der Deutschen Welle

(1) Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. *3*Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organes der Deutschen Welle. Die Tätigkeitsberichte übermittelt der Beauftragte auch der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

(5) Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. Die §§ 4f und 4g bleiben unberührt.

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnis-

mäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

§ 42b Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission

(1) Hält eine Aufsichtsbehörde einen Angemessenheitsbeschluss der Europäischen Kommission, einen Beschluss über die Anerkennung von Standardschutzklauseln oder über die Allgemeingültigkeit von genehmigten Verhaltensregeln, auf dessen Gültigkeit es für eine Entscheidung der Aufsichtsbehörde ankommt, für rechtswidrig, so hat die Aufsichtsbehörde ihr Verfahren auszusetzen und einen Antrag auf gerichtliche Entscheidung zu stellen.

(2) Für Verfahren nach Absatz 1 ist der Verwaltungsrechtsweg gegeben. Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 6 anzuwenden.

(3) Über einen Antrag der Aufsichtsbehörde nach Absatz 1 entscheidet im ersten und letzten Rechtszug das Bundesverwaltungsgericht.

(4) In Verfahren nach Absatz 1 ist die Aufsichtsbehörde beteiligungsfähig. An einem Verfahren nach Absatz 1 ist die Aufsichtsbehörde als Antragstellerin beteiligt; § 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt. Das Bundesverwaltungsgericht kann der Europäischen Kommission Gelegenheit zur Äußerung binnen einer zu bestimmenden Frist geben.

(5) Ist ein Verfahren zur Überprüfung der Gültigkeit eines Beschlusses der Europäischen Kommission nach Absatz 1 bei dem Gerichtshof der Europäischen Union anhängig, so kann das Bundesverwaltungsgericht anordnen, dass die Verhandlung bis zur Erledigung des Verfahrens vor dem Gerichtshof der Europäischen Union auszusetzen sei.

(6) In Verfahren nach Absatz 1 ist § 47 Absatz 5 Satz 1 und Absatz 6 der Verwaltungsgerichtsordnung entsprechend anzuwenden. Kommt das Bundesverwaltungsgericht zu der Überzeugung, dass der Beschluss der Europäischen Kommission nach Absatz 1 gültig ist, so stellt es dies in seiner Entscheidung fest. Andernfalls legt es die Frage nach der Gültigkeit des Beschlusses gemäß Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union dem Gerichtshof der Europäischen Union zur Entscheidung vor.

Fünfter Abschnitt Schlussvorschriften

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,

7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, ent-

gegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

§ 44 Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

Sechster Abschnitt Übergangsvorschriften

§ 45 Laufende Verwendungen

Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. Soweit Vorschriften dieses Gesetzes in Rechtsvorschriften außerhalb des Anwendungsbereichs 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 zur Anwendung gelangen, sind Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.

§ 46 Weitergeltung von Begriffsbestimmungen

(1) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder

2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(2) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Akte verwendet, ist Akte jede amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht dem Dateibegriff des Absatzes 1 unterfällt; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(3) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. Empfänger sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

§ 47 Übergangsregelung

Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 in der bis dahin geltenden Fassung weiter anzuwenden

1. für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,
2. für Zwecke der Werbung bis zum 31. August 2012.

§ 48 Bericht der Bundesregierung

Die Bundesregierung berichtet dem Bundestag

1. bis zum 31. Dezember 2012 über die Auswirkungen der §§ 30a und 42a,
2. bis zum 31. Dezember 2014 über die Auswirkungen der Änderungen der §§ 28 und 29.

Sofern sich aus Sicht der Bundesregierung gesetzgeberische Maßnahmen empfehlen, soll der Bericht einen Vorschlag enthalten.

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

   Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Anhang 4

Bundesdatenschutzgesetz neu

Art. 1 des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU – DSAnpUG-EU vom 30. Juni 2017, BGBl. I, S. 2097[1]

Nicht-amtliche Fassung

Inhaltsübersicht

[1] Das Gesetz tritt am 25. Mai 2018 in Kraft.

Kapitel 4

Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Kapitel 5

Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union

Kapitel 6

Rechtsbehelfe

Teil 2

Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679

Kapitel 1

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Abschnitt 1

Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken

Abschnitt 2
Besondere Verarbeitungssituationen

Kapitel 2

Rechte der betroffenen Person

Teil 3

Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

Kapitel 1

Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Kapitel 3

Rechte der betroffenen Person

Kapitel 4

Pflichten der Verantwortlichen und Auftragsverarbeiter

Teil 1

Gemeinsame Bestimmungen

Kapitel 1

Anwendungsbereich und Begriffsbestimmungen

§ 1

Anwendungsbereich des Gesetzes

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

   Für nichtöffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

(2) Andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(3) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) Dieses Gesetz findet Anwendung auf öffentliche Stellen. Auf nichtöffentliche Stellen findet es Anwendung, sofern

1. der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten im Inland verarbeitet,
2. die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer inländischen Niederlassung des Verantwortlichen oder Auftragsverarbeiters erfolgt oder

3. der Verantwortliche oder Auftragsverarbeiter zwar keine Niederlassung in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des

   Abkommens über den Europäischen Wirtschaftsraum hat, er aber in den Anwendungsbereich der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) fällt.

   Sofern dieses Gesetz nicht gemäß Satz 2 Anwendung findet, gelten für den Verantwortlichen oder Auftragsverarbeiter nur die §§ 8 bis 21, 39 bis 44.

(5) Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 in der jeweils geltenden Fassung, unmittelbar gilt.

(6) Bei Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittstaaten.

(7) Bei Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) stehen die bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands assoziierten Staaten den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittstaaten.

(8) Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten finden die Verordnung (EU) 2016/679 und die Teile 1 und 2 dieses Gesetzes entsprechend Anwendung, soweit nicht in diesem Gesetz oder einem anderen Gesetz Abweichendes geregelt ist.

§ 2

Begriffsbestimmungen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nichtöffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nichtöffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(5) Öffentliche Stellen des Bundes gelten als nichtöffentliche Stellen im Sinne dieses Gesetzes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Als nichtöffentliche Stellen im Sinne dieses Gesetzes gelten auch öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 3

Verarbeitung personenbezogener Daten durch öffentliche Stellen

Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

§ 4

Videoüberwachung öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,

2. zur Wahrnehmung des Hausrechts oder

3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei der Videoüberwachung von

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder

2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

(2) Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) Die Speicherung oder Verwendung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Absatz 1 Satz 2 gilt entsprechend. Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, so besteht die Pflicht zur Information der betroffenen Person über die Verarbeitung gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679. § 32 gilt entsprechend.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Kapitel 3

Datenschutzbeauftragte öffentlicher Stellen

§ 5

Benennung

(1) Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. Dies gilt auch für öffentliche Stellen nach § 2 Absatz 5, die am Wettbewerb teilnehmen.

(2) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter benannt werden.

(3) Die oder der Datenschutzbeauftragte wird auf der Grundlage ihrer oder seiner beruflichen Qualifikation und insbesondere ihres oder seines Fachwissens benannt, das sie oder er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer oder seiner Fähigkeit zur Erfüllung der in § 7 genannten Aufgaben.

(4) Die oder der Datenschutzbeauftragte kann Beschäftigte oder Beschäftigter der öffentlichen Stelle sein oder ihre oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(5) Die öffentliche Stelle veröffentlicht die Kontaktdaten der oder des Datenschutzbeauftragten und teilt diese Daten der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit.

§ 6

Stellung

(1) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Die öffentliche Stelle unterstützt die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben gemäß § 7, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung ihres oder seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

(3) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Die oder der Datenschutzbeauftragte berichtet unmittelbar der höchsten Leitungsebene der öffentlichen Stelle. Die oder der Datenschutzbeauftragte darf von der öffentlichen Stelle wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden.

(4) Die Abberufung der oder des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen.

Nach dem Ende der Tätigkeit als Datenschutzbeauftragte oder als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

(5) Betroffene Personen können die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der Verordnung (EU) 2016/679, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person befreit wird.

(6) Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

§ 7
Aufgaben

(1) Der oder dem Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) 2016/679 genannten Aufgaben zumindest folgende Aufgaben:

1. Unterrichtung und Beratung der öffentlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften;

2. Überwachung der Einhaltung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, sowie der Strategien der öffentlichen Stelle für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und der diesbezüglichen Überprüfungen;

3. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß § 67 dieses Gesetzes;

4. Zusammenarbeit mit der Aufsichtsbehörde;

5. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß § 69 dieses Gesetzes, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Im Fall einer oder eines bei einem Gericht bestellten Datenschutzbeauftragten beziehen sich diese Aufgaben nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit.

(2) Die oder der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die oder der Datenschutzbeauftragte trägt bei der Erfüllung ihrer oder seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie oder er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Kapitel 4

Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

§8

Errichtung

(1) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Bundesbeauftragte) ist eine oberste Bundesbehörde. Der Dienstsitz ist Bonn.

(2) Die Beamtinnen und Beamten der oder des Bundesbeauftragten sind Beamtinnen und Beamte des Bundes.

(3) Die oder der Bundesbeauftragte kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Bundes übertragen, soweit hierdurch die Unabhängigkeit der oder des Bundesbeauftragten nicht beeinträchtigt wird. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

§ 9

Zuständigkeit

(1) Die oder der Bundesbeauftragte ist zuständig für die Aufsicht über die öffentlichen Stellen des Bundes, auch soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Die Vorschriften dieses Kapitels gelten auch für Auftragsverarbeiter, soweit sie nichtöffentliche Stellen sind, bei denen dem Bund die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle des Bundes ist.

(2) Die oder der Bundesbeauftragte ist nicht zuständig für die Aufsicht über die von den Bundesgerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

§ 10

Unabhängigkeit

(1) Die oder der Bundesbeauftragte handelt bei der Erfüllung ihrer oder seiner Aufgaben und bei der Ausübung ihrer oder seiner Befugnisse völlig unabhängig. Sie oder er unterliegt weder direkter noch indirekter Beeinflussung von außen und ersucht weder um Weisung noch nimmt sie oder er Weisungen entgegen.

(2) Die oder der Bundesbeauftragte unterliegt der Rechnungsprüfung durch den Bundesrechnungshof, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

§ 11

Ernennung und Amtszeit

(1) Der Deutsche Bundestag wählt ohne Aussprache auf Vorschlag der Bundesregierung die Bundesbeauftragte oder den Bundesbeauftragten mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Die oder der Gewählte ist von der Bundespräsidentin oder dem Bundespräsidenten zu ernennen. Die oder der Bundesbeauftragte muss bei ihrer oder seiner Wahl das 35. Lebensjahr vollendet haben. Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Insbesondere muss die oder der Bundesbeauftragte über durch einschlägige Berufserfahrung erworbene Kenntnisse des Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Verwaltungsdienst haben.

(2) Die oder der Bundesbeauftragte leistet vor der Bundespräsidentin oder dem Bundespräsidenten folgenden Eid: „Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Ge-

rechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.“ Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit der oder des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

§ 12

Amtsverhältnis

(1) Die oder der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis.

(2) Das Amtsverhältnis beginnt mit der Aushändigung der Ernennungsurkunde. Es endet mit dem Ablauf der Amtszeit oder mit dem Rücktritt. Die Bundespräsidentin oder der Bundespräsident enthebt auf Vorschlag der Präsidentin oder des Präsidenten des Bundestages die Bundesbeauftragte ihres oder den Bundesbeauftragten seines Amtes, wenn die oder der Bundesbeauftragte eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Im Fall der Beendigung des Amtsverhältnisses oder der Amtsenthebung erhält die oder der Bundesbeauftragte eine von der Bundespräsidentin oder dem Bundespräsidenten vollzogene Urkunde. Eine Amtsenthebung wird mit der Aushändigung der Urkunde wirksam. Endet das Amtsverhältnis mit Ablauf der Amtszeit, ist die oder der Bundesbeauftragte verpflichtet, auf Ersuchen der Präsidentin oder des Präsidenten des Bundestages die Geschäfte bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers für die Dauer von höchstens sechs Monaten weiterzuführen.

(3) Die Leitende Beamtin oder der Leitende Beamte nimmt die Rechte der oder des Bundesbeauftragten wahr, wenn die oder der Bundesbeauftragte an der Ausübung ihres oder seines Amtes verhindert ist oder wenn ihr oder sein Amtsverhältnis endet und sie oder er nicht zur Weiterführung der Geschäfte verpflichtet ist. § 10 Absatz 1 ist entsprechend anzuwenden.

(4) Die oder der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Fall des Absatzes 2 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der Besoldungsgruppe B 11 sowie den Familienzuschlag entsprechend Anlage V des Bundesbesoldungsgesetzes. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im Übrigen sind § 12 Absatz 6 sowie die §§ 13 bis 20 und 21a Absatz 5 des Bundesministergesetzes mit den Maßgaben anzuwenden, dass an die Stelle der vierjährigen Amtszeit in § 15 Absatz 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 und 21a Absatz 5 des Bundesministergesetzes berechnet sich das Ruhegehalt der oder des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige

Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und die oder der Bundesbeauftragte sich unmittelbar vor ihrer oder seiner Wahl zur oder zum Bundesbeauftragten als Beamtin oder Beamter oder als Richterin oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 11 zu durchlaufenden Amt befunden hat.

§ 13

Rechte und Pflichten

(1) Die oder der Bundesbeauftragte sieht von allen mit den Aufgaben ihres oder seines Amtes nicht zu vereinbarenden Handlungen ab und übt während ihrer oder seiner Amtszeit keine andere mit ihrem oder seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. Insbesondere darf die oder der Bundesbeauftragte neben ihrem oder seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Sie oder er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(2) Die oder der Bundesbeauftragte hat der Präsidentin oder dem Präsidenten des Bundestages Mitteilung über Geschenke zu machen, die sie oder er in Bezug auf das Amt erhält. Die Präsidentin oder der Präsident des Bundestages entscheidet über die Verwendung der Geschenke. Sie oder er kann Verfahrensvorschriften erlassen.

(3) Die oder der Bundesbeauftragte ist berechtigt, über Personen, die ihr oder ihm in ihrer oder seiner Eigenschaft als Bundesbeauftragte oder Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiterinnen und Mitarbeiter der oder des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts die oder der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht der oder des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Dokumenten von ihr oder ihm nicht gefordert werden.

(4) Die oder der Bundesbeauftragte ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die oder der Bundesbeauftragte entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie oder er über solche Angelegenheiten vor Gericht oder außergerichtlich aussagt oder Erklärungen abgibt; wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Bundesbeauftragten erforderlich. Unberührt

bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei einer Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. Für die Bundesbeauftragte oder den Bundesbeauftragten und ihre oder seine Mitarbeiterinnen und Mitarbeiter gelten die §§ 93, 97 und 105 Absatz 1, § 111 Absatz 5 in Verbindung mit § 105 Absatz 1 sowie § 116 Absatz 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben der oder des Auskunftspflichtigen oder der für sie oder ihn tätigen Personen handelt. Stellt die oder der Bundesbeauftragte einen Datenschutzverstoß fest, ist sie oder er befugt, diesen anzuzeigen und die betroffene Person hierüber zu informieren.

(5) Die oder der Bundesbeauftragte darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde

1. dem Wohl des Bundes oder eines Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit der Bundesrepublik Deutschland oder ihre Beziehungen zu anderen Staaten, oder

2. Grundrechte verletzen.

Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Bundesregierung zuzurechnen sind oder sein könnten, darf die oder der Bundesbeauftragte nur im Benehmen mit der Bundesregierung aussagen. § 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.

(6) Die Absätze 3 und 4 Satz 5 bis 7 gelten entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 14
Aufgaben

(1) Die oder der Bundesbeauftragte hat neben den in der Verordnung (EU) 2016/679 genannten Aufgaben die Aufgaben,

1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu überwachen und durchzusetzen,

2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Maßnahmen für Kinder besondere Beachtung finden,

3. den Deutschen Bundestag und den Bundesrat, die Bundesregierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,

4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten zu sensibilisieren,

5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Vorschriften über den Daten-schutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenzuarbeiten,

6. sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 55 der Richtlinie (EU) 2016/680 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,

7. mit anderen Aufsichtsbehörden zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu gewährleisten,

8. Untersuchungen über die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde,

9. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken,

10. Beratung in Bezug auf die in § 69 genannten Verarbeitungsvorgänge zu leisten und

11. Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses zu leisten.

Im Anwendungsbereich der Richtlinie (EU) 2016/680 nimmt die oder der Bundesbeauftragte zudem die Aufgabe nach § 60 wahr.

(2) Zur Erfüllung der in Absatz 1 Satz 1 Nummer 3 genannten Aufgabe kann die oder der Bundes-

beauftragte zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an den Deutschen Bundestag oder einen seiner Ausschüsse, den Bundesrat, die Bundesregierung, sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit richten. Auf Ersuchen des Deutschen Bundestages, eines seiner Ausschüsse oder der Bundesregierung geht die oder der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach.

(3) Die oder der Bundesbeauftragte erleichtert das Einreichen der in Absatz 1 Satz 1 Nummer 6 genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(4) Die Erfüllung der Aufgaben der oder des Bundesbeauftragten ist für die betroffene Person unentgeltlich. Bei offenkundig unbegründeten oder, insbesondere im Fall von häufiger Wiederholung, exzessiven Anfragen kann die oder der Bundesbeauftragte eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die oder der Bundesbeauftragte die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

§ 15

Tätigkeitsbericht

Die oder der Bundesbeauftragte erstellt einen Jahresbericht über ihre oder seine Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen, einschließlich der verhängten Sanktionen und der Maßnahmen nach Artikel 58 Absatz 2 der Verordnung (EU) 2016/679, enthalten kann. Die oder der Bundesbeauftragte übermittelt den Bericht dem Deutschen Bundestag, dem Bundesrat und der Bundesregierung und macht ihn der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich.

§ 16

Befugnisse

(1) Die oder der Bundesbeauftragte nimmt im Anwendungsbereich der Verordnung (EU) 2016/679 die Befugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 wahr. Kommt die oder der Bundesbeauftragte zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie oder er dies der zuständigen Rechts- oder Fachaufsichtsbehörde mit und gibt dieser vor der Ausübung der Befugnisse des Artikels 58 Absatz 2 Buchstabe b bis g, i und j der Verordnung (EU) 2016/679 gegenüber dem Verantwortlichen Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. Von der Einräumung der Gelegenheit zur

Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Bundesbeauftragten getroffen worden sind.

(2) Stellt die oder der Bundesbeauftragte bei Datenverarbeitungen durch öffentliche Stellen des Bundes zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies gegenüber der zuständigen obersten Bundesbehörde und fordert diese zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auf. Die oder der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Bundesbeauftragten getroffen worden sind. Die oder der Bundesbeauftragte kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen.

(3) Die Befugnisse der oder des Bundesbeauftragten erstrecken sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs und

2. personenbezogene Daten, die einem besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, der oder dem Bundesbeauftragten und ihren oder seinen Beauftragten

1. jederzeit Zugang zu den Grundstücken und Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer oder seiner Aufgaben notwendig sind, zu gewähren und

2. alle Informationen, die für die Erfüllung ihrer oder seiner Aufgaben erforderlich sind, bereitzustellen.

(5) Die oder der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern

zuständig sind, sowie mit den Aufsichtsbehörden nach § 40 hin. § 40 Absatz 3 Satz 1 zweiter Halbsatz gilt entsprechend.

Kapitel 5

Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union

§ 17

Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

(1) Gemeinsamer Vertreter im Europäischen Datenschutzausschuss und zentrale Anlaufstelle ist die oder der Bundesbeauftragte (gemeinsamer Vertreter). Als Stellvertreterin oder Stellvertreter des gemeinsamen Vertreters wählt der Bundesrat eine Leiterin oder einen Leiter der Aufsichtsbehörde eines Landes (Stellvertreter). Die Wahl erfolgt für fünf Jahre. Mit dem Ausscheiden aus dem Amt als Leiterin oder Leiter der Aufsichtsbehörde eines Landes endet zugleich die Funktion als Stellvertreter. Wiederwahl ist zulässig.

(2) Der gemeinsame Vertreter überträgt in Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche die Länder allein das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, dem Stellvertreter auf dessen Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss.

§ 18

Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder

(1) Die oder der Bundesbeauftragte und die Aufsichtsbehörden der Länder (Aufsichtsbehörden des Bundes und der Länder) arbeiten in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 zusammen. Vor der Übermittlung eines gemeinsamen Standpunktes an die Aufsichtsbehörden der anderen Mitgliedstaaten, die Europäische Kommission oder den Europäischen Datenschutzausschuss geben sich die Aufsichtsbehörden des Bundes und der Länder frühzeitig Gelegenheit zur Stellungnahme. Zu diesem Zweck tauschen sie untereinander alle zweckdienlichen Informationen aus. Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach den Artikeln 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.

(2) Soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, legen die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter einen Vorschlag für einen ge-

meinsamen Standpunkt vor. Einigen sich der gemeinsame Vertreter und sein Stellvertreter nicht auf einen Vorschlag für einen gemeinsamen Standpunkt, legt in Angelegenheiten, die die Wahrnehmung von Aufgaben betreffen, für welche die Länder allein das Recht der Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, der Stellvertreter den Vorschlag für einen gemeinsamen Standpunkt fest. In den übrigen Fällen fehlenden Einvernehmens nach Satz 2 legt der gemeinsame Vertreter den Standpunkt fest. Der nach den Sätzen 1 bis 3 vorgeschlagene Standpunkt ist den Verhandlungen zu Grunde zu legen, wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen. Der Bund und jedes Land haben jeweils eine Stimme. Enthaltungen werden nicht gezählt.

(3) Der gemeinsame Vertreter und dessen Stellvertreter sind an den gemeinsamen Stand-punkt nach den Absätzen 1 und 2 gebunden und legen unter Beachtung dieses Standpunktes einvernehmlich die jeweilige Verhandlungsführung fest. Sollte ein Einvernehmen nicht erreicht werden, entscheidet in den in § 18 Absatz 2 Satz 2 genannten Angelegenheiten der Stellvertreter über die weitere Verhandlungsführung. In den übrigen Fällen gibt die Stimme des gemeinsamen Vertreters den Ausschlag.

§ 19

Zuständigkeiten

(1) Federführende Aufsichtsbehörde eines Landes im Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII der Verordnung (EU) 2016/679 ist die Aufsichtsbehörde des Landes, in dem der Verantwortliche oder der Auftragsverarbeiter seine Hauptniederlassung im Sinne des Artikels 4 Nummer 16 der Verordnung (EU) 2016/679 oder seine einzige Niederlassung in der Europäischen Union im Sinne des Artikels 56 Absatz 1 der Verordnung (EU) 2016/679 hat. Im Zuständigkeitsbereich der oder des Bundesbeauftragten gilt Artikel 56 Absatz 1 in Verbindung mit Artikel 4 Nummer 16 der Verordnung (EU) 2016/679 entsprechend. Besteht über die Federführung kein Einvernehmen, findet für die Festlegung der federführenden Aufsichtsbehörde das Verfahren des § 18 Absatz 2 entsprechende Anwendung.

(2) Die Aufsichtsbehörde, bei der eine betroffene Person Beschwerde eingereicht hat, gibt die Beschwerde an die federführende Aufsichtsbehörde nach Absatz 1, in Ermangelung einer solchen an die Aufsichtsbehörde eines Landes ab, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wird eine Beschwerde bei einer sachlich unzuständigen Aufsichtsbehörde eingereicht, gibt diese, sofern eine Abgabe nach Satz 1 nicht in Betracht kommt, die Beschwerde an die Aufsichtsbehörde am Wohnsitz des Beschwerdeführers ab. Die empfangende Aufsichtsbehörde gilt als die Aufsichtsbehörde nach Maßgabe des Kapitels VII der Verordnung (EU) 2016/679, bei der die Beschwerde eingereicht worden ist, und kommt den Verpflichtungen aus Artikel 60 Absatz 7 bis 9 und Artikel 65 Absatz 6 der Verordnung (EU) 2016/679 nach.

Kapitel 6

Rechtsbehelfe

§ 20

Gerichtlicher Rechtsschutz

(1) Für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und einer Aufsichtsbehörde des Bundes oder eines Landes über Rechte gemäß Artikel 78 Absatz 1 und 2 der Verordnung (EU) 2016/679 sowie § 61 ist der Verwaltungsrechtsweg gegeben. Satz 1 gilt nicht für Bußgeldverfahren.

(2) Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 7 anzuwenden.

(3) Für Verfahren nach Absatz 1 Satz 1 ist das Verwaltungsgericht örtlich zuständig, in dessen Bezirk die Aufsichtsbehörde ihren Sitz hat.

(4) In Verfahren nach Absatz 1 Satz 1 ist die Aufsichtsbehörde beteiligungsfähig.

(5) Beteiligte eines Verfahrens nach Absatz 1 Satz 1 sind

1. die natürliche oder juristische Person als Klägerin oder Antragstellerin und
2. die Aufsichtsbehörde als Beklagte oder Antragsgegnerin.

§ 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt.

(6) Ein Vorverfahren findet nicht statt.

(7) Die Aufsichtsbehörde darf gegenüber einer Behörde oder deren Rechtsträger nicht die sofortige Vollziehung gemäß § 80 Absatz 2 Satz 1 Nummer 4 der Verwaltungsgerichtsordnung anordnen.

§ 21

Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission

(1) Hält eine Aufsichtsbehörde einen Angemessenheitsbeschluss der Europäischen Kommission, einen Beschluss über die Anerkennung von Standardschutzklauseln oder über die Allgemeingültigkeit von genehmigten Verhaltensregeln, auf dessen Gültigkeit es für eine Entscheidung der Aufsichtsbehörde ankommt, für rechtswidrig, so hat die Aufsichtsbehörde ihr Verfahren auszusetzen und einen Antrag auf gerichtliche Entscheidung zu stellen.

(2) Für Verfahren nach Absatz 1 ist der Verwaltungsrechtsweg gegeben. Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 6 anzuwenden.

(3) Über einen Antrag der Aufsichtsbehörde nach Absatz 1 entscheidet im ersten und letzten Rechtszug das Bundesverwaltungsgericht.

(4) In Verfahren nach Absatz 1 ist die Aufsichtsbehörde beteiligungsfähig. An einem Verfahren nach Absatz 1 ist die Aufsichtsbehörde als Antragstellerin beteiligt; § 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt. Das Bundesverwaltungsgericht kann der Europäischen Kommission Gelegenheit zur Äußerung binnen einer zu bestimmenden Frist geben.

(5) Ist ein Verfahren zur Überprüfung der Gültigkeit eines Beschlusses der Europäischen Kommission nach Absatz 1 bei dem Gerichtshof der Europäischen Union anhängig, so kann das Bundesverwaltungsgericht anordnen, dass die Verhandlung bis zur Erledigung des Verfahrens vor dem Gerichtshof der Europäischen Union auszusetzen sei.

(6) In Verfahren nach Absatz 1 ist § 47 Absatz 5 Satz 1 und Absatz 6 der Verwaltungsgerichtsordnung entsprechend anzuwenden. Kommt das Bundesverwaltungsgericht zu der Überzeugung, dass der Beschluss der Europäischen Kommission nach Absatz 1 gültig ist, so stellt es dies in seiner Entscheidung fest. Andernfalls legt es die Frage nach der Gültigkeit des Beschlusses gemäß Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union dem Gerichtshof der Europäischen Union zur Entscheidung vor.

Teil 2

Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679

Kapitel 1

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Abschnitt 1

Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken

§ 22

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig

1. durch öffentliche und nichtöffentliche Stellen, wenn sie

   a) erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen,

   b) zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder

   c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Absatz 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten,

2. durch öffentliche Stellen, wenn sie

   a) aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist,

   b) zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,

   c) zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist oder

   d) aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist

   und soweit die Interessen des Verantwortlichen an der Datenverarbeitung in den Fällen der Nummer 2 die Interessen der betroffenen Person überwiegen.

(2) In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,

2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,

3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

4. Benennung einer oder eines Datenschutzbeauftragten,

5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,

6. Pseudonymisierung personenbezogener Daten,

7. Verschlüsselung personenbezogener Daten,

8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder

10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.

§ 23

Verarbeitung zu anderen Zwecken durch öffentliche Stellen

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen,

zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,

2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

3. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher

Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,

4. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im

   Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,

5. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

6. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Absatzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

§ 24

Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen ist zulässig, wenn

1. sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder

2. sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist,

   sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Absatzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

§ 25

Datenübermittlungen durch öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 23 zulassen würden.

Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist unter den Voraussetzungen des § 23 zulässig.

(2) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nichtöffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 23 zulassen würden,

2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder

3. es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist

und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

(3) Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 ist zulässig, wenn die Voraussetzungen des Absatzes 1 oder 2 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

Abschnitt 2

Besondere Verarbeitungssituationen

§ 26

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines

Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechten und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

(3) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 22 Absatz 2 gilt entsprechend.

(4) Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(6) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(8) Beschäftigte im Sinne dieses Gesetzes sind:

1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

§ 27

Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere

Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(4) Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 28

Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(3) Das Recht auf Berichtigung der betroffenen Person gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

(4) Die in Artikel 18 Absatz 1 Buchstabe a, b und d, den Artikeln 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

§ 29

Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Die Pflicht zur Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 3 ist die betroffene Person nach Artikel 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

(2) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

(3) Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.

§ 30

Verbraucherkredite

(1) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(2) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 1 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 37 bleibt unberührt.

§ 31

Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften

(1) Die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (Scoring) ist nur zulässig, wenn

1. die Vorschriften des Datenschutzrechts eingehalten wurden,

2. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,

3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt wurden und

4. im Fall der Nutzung von Anschriftendaten die betroffene Person vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

(2) Die Verwendung eines von Auskunfteien ermittelten Wahrscheinlichkeitswerts über die Zahlungsfähig- und Zahlungswilligkeit einer natürlichen Person ist im Fall der Einbeziehung von Informationen über Forderungen nur zulässig, soweit die Voraussetzungen nach Absatz 1 vorliegen und nur solche Forderungen über eine geschuldete Leistung, die trotz Fälligkeit nicht erbracht worden ist, berücksichtigt werden,

1. die durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden sind oder für die ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden sind,

3. die der Schuldner ausdrücklich anerkannt hat,

4. bei denen

   a) der Schuldner nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

   b) die erste Mahnung mindestens vier Wochen zurückliegt,

   c) der Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist und

   d) der Schuldner die Forderung nicht bestritten hat oder

5. deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist.

Die Zulässigkeit der Verarbeitung, einschließlich der Ermittlung von Wahrscheinlichkeitswerten, von anderen bonitätsrelevanten Daten nach allgemeinem Datenschutzrecht bleibt unberührt.

Kapitel 2

Rechte der betroffenen Person

§ 32

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

1. eine Weiterverarbeitung analog gespeicherter Daten betrifft, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem ursprünglichen Erhebungszweck gemäß der Verordnung (EU) 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist,

2. im Fall einer öffentlichen Stelle die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 gefährden würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen,

3. die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen,

4. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder

5. eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat. Die Sätze 1 und 2 finden in den Fällen des Absatzes 1 Nummer 4 und 5 keine Anwendung.

(3) Unterbleibt die Benachrichtigung in den Fällen des Absatzes 1 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Fortfall des Hinderungsgrundes, spätestens jedoch innerhalb von zwei Wochen, nach.

§ 33

Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und der in § 29 Absatz 1 Satz 1 genannten Ausnahme nicht, wenn die Erteilung der Information

1. im Fall einer öffentlichen Stelle

   a) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 gefährden würde oder

b) die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss,

2. im Fall einer nichtöffentlichen Stelle

a) die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher An-sprüche beeinträchtigen würde oder die Verarbeitung Daten aus zivil-rechtlichen Verträgen beinhaltet und der Verhütung von Schäden durch Straftaten dient, sofern nicht das berechtigte Interesse der betroffenen Person an der Informationserteilung überwiegt, oder

b) die zuständige öffentliche Stelle gegenüber dem Verantwortlichen fest-gestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde; im Fall der Datenverarbeitung für Zwecke der Strafverfolgung bedarf es keiner Feststellung nach dem ersten Halbsatz.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat.

(3) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten durch öffentliche Stellen an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

§ 34

Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht ergänzend zu den in § 27 Absatz 2, § 28 Absatz 2 und § 29 Absatz 1 Satz 2 genannten Ausnahmen nicht, wenn

1. die betroffene Person nach § 33 Absatz 1 Nummer 1, 2 Buchstabe b oder Absatz 3 nicht zu informieren ist, oder

2. die Daten

   a) nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder

   b) ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen

   und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(2) Die Gründe der Auskunftsverweigerung sind zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Artikels 18 der Verordnung (EU) 2016/679 einzuschränken.

(3) Wird der betroffenen Person durch eine öffentliche Stelle des Bundes keine Auskunft erteilt, so ist sie auf ihr Verlangen der oder dem Bundesbeauftragten zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Bundesbeauftragten an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

(4) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

§ 35

Recht auf Löschung

(1) Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung

personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

(2) Ergänzend zu Artikel 18 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 gilt Absatz 1 Satz 1 und 2 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a und d der Verordnung (EU) 2016/679, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu Artikel 17 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 gilt Absatz 1 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679, wenn einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen.

§ 36

Widerspruchsrecht

Das Recht auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

§ 37

Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und

1. dem Begehren der betroffenen Person stattgegeben wurde oder

2. die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Stand-

punktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens zum Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird.

(2) Entscheidungen nach Absatz 1 dürfen auf der Verarbeitung von Gesundheitsdaten im Sinne des Artikels 4 Nummer 15 der Verordnung (EU) 2016/679 beruhen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

Kapitel 3

Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 38

Datenschutzbeauftragte nichtöffentlicher Stellen

(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

§ 39

Akkreditierung

Die Erteilung der Befugnis, als Zertifizierungsstelle gemäß Artikel 43 Absatz 1 Satz 1 der Verordnung (EU) 2016/679 tätig zu werden, erfolgt durch die für die datenschutzrechtliche Aufsicht über die Zertifizierungsstelle zuständige Aufsichtsbehörde des Bundes oder der Länder auf der Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle. § 2 Absatz 3 Satz 2, § 4 Absatz 3 und § 10 Absatz 1 Satz 1 Nummer 3 des Akkreditierungsstellengesetzes finden mit der Maßgabe Anwendung, dass der Datenschutz als ein dem Anwendungsbereich des § 1 Absatz 2 Satz 2 unterfallender Bereich gilt.

Kapitel 4

Aufsichtsbehörde für die Datenverarbeitung durch nichtöffentliche Stellen

§ 40

Aufsichtsbehörden der Länder

(1) Die nach Landesrecht zuständigen Behörden überwachen im Anwendungsbereich der Verordnung (EU) 2016/679 bei den nichtöffentlichen Stellen die Anwendung der Vorschriften über den Datenschutz.

(2) Hat der Verantwortliche oder Auftragsverarbeiter mehrere inländische Niederlassungen, findet für die Bestimmung der zuständigen Aufsichtsbehörde Artikel 4 Nummer 16 der Verordnung (EU) 2016/679 entsprechende Anwendung. Wenn sich mehrere Behörden für zuständig oder für unzuständig halten oder wenn die Zuständigkeit aus anderen Gründen zweifelhaft ist, treffen die Aufsichtsbehörden die Entscheidung gemeinsam nach Maßgabe des § 18 Absatz 2. § 3 Absatz 3 und 4 des Verwaltungsverfahrensgesetzes findet entsprechende Anwendung.

(3) Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten; hierbei darf sie Daten an andere Aufsichtsbehörden übermitteln. Eine Verarbeitung zu einem anderen Zweck ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,

2. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist oder

3. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist.

Stellt die Aufsichtsbehörde einen Verstoß gegen die Vorschriften über den Datenschutz fest, so ist sie befugt, die betroffenen Personen hierüber zu unterrichten, den Verstoß anderen für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. § 13 Absatz 4 Satz 4 bis 7 gilt entsprechend.

(4) Die der Aufsicht unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben einer Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Absatz 1 Nummer 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(5) Die von einer Aufsichtsbehörde mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen sind befugt, zur Erfüllung ihrer Aufgaben Grundstücke und Geschäftsräume der Stelle zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geraten zu erhalten. Die Stelle ist insoweit zur Duldung verpflichtet. § 16 Absatz 4 gilt entsprechend.

(6) Die Aufsichtsbehörden beraten und unterstützen die Datenschutzbeauftragten mit Rücksicht auf deren typische Bedürfnisse. Sie können die Abberufung der oder des Datenschutzbeauftragten verlangen, wenn sie oder er die zur Erfüllung ihrer oder seiner Aufgaben erforderliche Fachkunde nicht besitzt oder im Fall des Artikels 38 Absatz 6 der Verordnung (EU) 2016/679 ein schwerwiegender Interessenkonflikt vorliegt.

(7) Die Anwendung der Gewerbeordnung bleibt unberührt.

Kapitel 5

Sanktionen

§ 41

Anwendung der Vorschriften über das Bußgeld- und Strafverfahren

(1) Für Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. § 68 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass das Landgericht entscheidet, wenn die festgesetzte Geldbuße den Betrag von einhunderttausend Euro übersteigt.

(2) Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes, entsprechend. Die §§ 56 bis 58, 87, 88, 99 und 100 des Gesetzes über Ordnungswidrigkeiten finden keine

Anwendung. § 69 Absatz 4 Satz 2 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass die Staatsanwaltschaft das Verfahren nur mit Zustimmung der Aufsichtsbehörde, die den Bußgeldbescheid erlassen hat, einstellen kann.

§ 42
Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43
Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder
2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Kapitel 6

Rechtsbehelfe

§ 44

Klagen gegen den Verantwortlichen oder Auftragsverarbeiter

(1) Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 oder der darin enthaltenen Rechte der betroffenen Person können bei dem Gericht des Ortes erhoben werden, an dem sich eine Niederlassung des Verantwortlichen oder Auftragsverarbeiters befindet. Klagen nach Satz 1 können auch bei dem Gericht des Ortes erhoben werden, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat.

(2) Absatz 1 gilt nicht für Klagen gegen Behörden, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden sind.

(3) Hat der Verantwortliche oder Auftragsverarbeiter einen Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt, gilt dieser auch als bevollmächtigt, Zustellungen in zivilgerichtlichen Verfahren nach Absatz 1 entgegenzunehmen. § 184 der Zivilprozessordnung bleibt unberührt.

Teil 3

Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

Kapitel 1

Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

§ 45

Anwendungsbereich

Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche. Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. Die Sätze 1 und 2 finden zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen, von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind. Soweit dieser Teil Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.

§ 46

Begriffsbestimmungen

Es bezeichnen die Begriffe:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Über-

mittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können;

6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden;

11. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden;

12. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;

13. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

14. „besondere Kategorien personenbezogener Daten“

    a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

    b) genetische Daten,

    c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

    d) Gesundheitsdaten und

    e) Daten zum Sexualleben oder zur sexuellen Orientierung;

15. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle;

16. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen sowie jede sonstige Einrichtung, die durch eine von zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;

17. „Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

§ 47

Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck stehen,
4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,
5. nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, und
6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 48

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

(2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen. Geeignete Garantien können insbesondere sein

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,
2. die Festlegung von besonderen Aussonderungsprüffristen,

3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle,

5. die von anderen Daten getrennte Verarbeitung,

6. die Pseudonymisierung personenbezogener Daten,

7. die Verschlüsselung personenbezogener Daten oder

8. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

§ 49

Verarbeitung zu anderen Zwecken

Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 45 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten, und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 45 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

§ 50

Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken

Personenbezogene Daten dürfen im Rahmen der in § 45 genannten Zwecke in archivarischer, wissenschaftlicher oder statistischer Form verarbeitet werden, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden. Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.

§ 51

Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und

leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

(4) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

(5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

§ 52

Verarbeitung auf Weisung des Verantwortlichen

Jede einem Verantwortlichen oder einem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist.

§ 53

Datengeheimnis

Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

§ 54

Automatisierte Einzelentscheidung

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(2) Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

(3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

Kapitel 3

Rechte der betroffenen Person

§ 55

Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke der von ihm vorgenommenen Verarbeitungen,
2. die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,
3. den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten,
4. das Recht, die Bundesbeauftragte oder den Bundesbeauftragten anzurufen, und
5. die Erreichbarkeit der oder des Bundesbeauftragten.

§ 56

Benachrichtigung betroffener Personen

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. die in § 55 genannten Angaben,
2. die Rechtsgrundlage der Verarbeitung,
3. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie
5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 kann der Verantwortliche die Benachrichtigung insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls

1. die Erfüllung der in § 45 genannten Aufgaben,
2. die öffentliche Sicherheit oder
3. Rechtsgüter Dritter

gefährdet würden, wenn das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Fall der Einschränkung nach Absatz 2 gilt § 57 Absatz 7 entsprechend.

§ 57

Auskunftsrecht

(1) Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,
2. die verfügbaren Informationen über die Herkunft der Daten,
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,
5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,
7. das Recht nach § 60, die Bundesbeauftragte oder den Bundesbeauftragten anzurufen, sowie
8. Angaben zur Erreichbarkeit der oder des Bundesbeauftragten.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Von der Auskunftserteilung ist abzusehen, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 56 Absatz 2 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 2 teilweise oder vollständig einschränken.

(5) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 56 Absatz 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

(7) Wird die betroffene Person nach Absatz 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Bundesbeauftragte oder den Bundesbeauftragten ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäß § 60 die Bundesbeauftragte oder den Bundesbeauftragten anrufen oder gerichtlichen Rechtsschutz suchen kann. Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Bundesbeauftragten zu erteilen, soweit nicht die zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die oder der Bundesbeauftragte hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung der oder des Bundesbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Der

Verantwortliche darf die Zustimmung nur insoweit und solange verweigern, wie er nach Absatz 4 von einer Auskunft absehen oder sie einschränken könnte. Die oder der Bundesbeauftragte hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(8) Der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

§ 58

Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,

2. die Daten zu Beweiszwecken in Verfahren, die Zwecken des § 45 dienen, weiter aufbewahrt werden müssen oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand.

(4) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(5) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

(6) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 56 Absatz 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.

(7) § 57 Absatz 7 und 8 findet entsprechende Anwendung.

§ 59

Verfahren für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwenden.

(2) Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 57 Absatz 6 und des § 58 Absatz 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.

(3) Die Erteilung von Informationen nach § 55, die Benachrichtigungen nach den §§ 56 und 66 und die Bearbeitung von Anträgen nach den §§ 57 und 58 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 57 und 58 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 57 oder 58 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 60

Anrufung der oder des Bundesbeauftragten

(1) Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Bundesbeauftragte oder den Bundesbeauftragten wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen zu den in § 45 genannten Zwecken in ihren Rechten verletzt worden zu sein. Dies gilt nicht für die Verarbeitung von personenbezogenen Daten durch Gerichte, soweit diese die Daten im Rahmen ihrer justiziellen Tätigkeit verarbeitet haben. Die oder der Bundesbeauftragte hat die betroffene Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 61 hinzuweisen.

(2) Die oder der Bundesbeauftragte hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde des anderen Staates weiterzuleiten. Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

§ 61

Rechtsschutz gegen Entscheidungen der oder des Bundesbeauftragten oder bei deren oder dessen Untätigkeit

(1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen eine verbindliche Entscheidung der oder des Bundesbeauftragten vorgehen.

(2) Absatz 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Bundesbeauftragte mit einer Beschwerde nach § 60 nicht befasst oder die betroffene Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

Kapitel 4

Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 62

Auftragsverarbeitung

(1) Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. Die Rechte

der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

(3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

(4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(5) Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren;

2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;

4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;

5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 76 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;

6. Überprüfungen, die von dem Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;

7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

8. alle gemäß § 64 erforderlichen Maßnahmen ergreift und

9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 64 bis 67 und § 69 genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Absatzes 5 ist schriftlich oder elektronisch abzufassen.

(7) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

§ 63

Gemeinsam Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam Verantwortliche. Gemeinsam Verantwortliche haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können. Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

§ 64

Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit

der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und

2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),

10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),

11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),

12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet wer—den, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 65

Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten

(1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Bundesbeauftragten zu melden, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat. Erfolgt die Meldung an die Bundesbeauftragte oder den Bundesbeauftragten nicht innerhalb von 72 Stunden, so ist die Verzögerung zu begründen.

(2) Ein Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden.

(3) Die Meldung nach Absatz 1 hat zumindest folgende Informationen zu enthalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Per-

sonen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,

2. den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,

3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung und der getroffenen Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, hat der Verantwortliche sie unverzüglich nachzureichen, sobald sie ihm vorliegen.

(5) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Absatz 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) § 42 Absatz 4 findet entsprechende Anwendung.

(8) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

§ 66

Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich über den Vorfall zu benachrichtigen.

(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 65 Absatz 3 Nummer 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.

(3) Von der Benachrichtigung nach Absatz 1 kann abgesehen werden, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen

getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden;

2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach keine erhebliche Gefahr im Sinne des Absatzes 1 mehr besteht, oder

3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die oder der Bundesbeauftragte förmlich feststellen, dass ihrer oder seiner Auffassung nach die in Absatz 3 genannten Voraussetzungen nicht erfüllt sind. Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, dass die Verletzung eine erhebliche Gefahr im Sinne des Absatzes 1 zur Folge hat.

(5) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in § 56 Absatz 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden erheblichen Gefahr im Sinne des Absatzes 1 überwiegen.

(6) § 42 Absatz 4 findet entsprechende Anwendung.

§ 67

Durchführung einer Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche hat die Datenschutzbeauftragte oder den Datenschutzbeauftragten an der Durchführung der Folgenabschätzung zu beteiligen.

(4) Die Folgenabschätzung hat den Rechten der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,

2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,

3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und

4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, ein-schließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

(5) Soweit erforderlich, hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben.

§ 68

Zusammenarbeit mit der oder dem Bundesbeauftragten

Der Verantwortliche hat mit der oder dem Bundesbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

§ 69

Anhörung der oder des Bundesbeauftragten

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Bundesbeauftragte oder den Bundesbeauftragten anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 67 hervorgeht, dass die Verarbeitung eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde, oder

2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hat.

Die oder der Bundesbeauftragte kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

(2) Der oder dem Bundesbeauftragten sind im Fall des Absatzes 1 vorzulegen:

1. die nach § 67 durchgeführte Datenschutz-Folgenabschätzung,

2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,

3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,

4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Personen vorgesehenen Maßnahmen und Garantien und

5. Name und Kontaktdaten der oder des Datenschutzbeauftragten.

Auf Anforderung sind ihr oder ihm zudem alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(3) Falls die oder der Bundesbeauftragte der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Die oder der Bundesbeauftragte kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. Sie oder er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren.

(4) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 3 Satz 1 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Bundesbeauftragten im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

§ 70

Verzeichnis von Verarbeitungstätigkeiten

(1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten,

2. die Zwecke der Verarbeitung,

3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,

4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,

5. gegebenenfalls die Verwendung von Profiling,

6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,

7. Angaben über die Rechtsgrundlage der Verarbeitung,

8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und

9. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 64.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt, das Folgendes zu enthalten hat:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls der oder des Datenschutzbeauftragten,

2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates oder der Organisation und

3. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 64.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch zu führen.

(4) Verantwortliche und Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse der oder dem Bundesbeauftragten zur Verfügung zu stellen.

§ 71

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten

und die Rechte der betroffenen Personen geschützt werden. Er hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

(2) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

§ 72

Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,
2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,
3. verurteilte Straftäter,
4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und
5. andere Personen wie insbesondere Zeugen, Hinweisgeber oder Personen, die mit den in den Nummern 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

§ 73

Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

Der Verantwortliche hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 74

Verfahren bei Übermittlungen

(1) Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht über-mittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

§ 75

Berichtigung und Löschung personenbezogener Daten
sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind.

(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

(3) § 58 Absatz 3 bis 5 ist entsprechend anzuwenden. Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist auch dies dem Empfänger mitzuteilen.

(4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

§ 76

Protokollierung

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,
2. Veränderung,
3. Abfrage,
4. Offenlegung einschließlich Übermittlung,
5. Kombination und
6. Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die Bundesbeauftragte oder den Bundesbeauftragten und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

(4) Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.

(5) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Bundesbeauftragten auf Anforderung zur Verfügung zu stellen.

§ 77

Vertrauliche Meldung von Verstößen

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

Kapitel 5

Datenübermittlungen an Drittstaaten und an internationale Organisationen

§ 78

Allgemeine Voraussetzungen

(1) Die Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die in § 45 genannten Zwecke zuständig ist und

2. die Europäische Kommission gemäß Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

(2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Absatzes 1 Nummer 2 und des zu berücksichtigenden öffentlichen Interesses an der Datenübermittlung zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Bei seiner Beurteilung hat der Verantwortliche maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satzes 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung

der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

(4) Der Verantwortliche, der Daten nach Absatz 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder die andere internationale Organisation zulässig wäre. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 79

Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 78 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 78 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

2. der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche hat Übermittlungen nach Absatz 1 Nummer 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist der oder dem Bundesbeauftragten auf Anforderung zur Verfügung zu stellen.

(3) Der Verantwortliche hat die Bundesbeauftragte oder den Bundesbeauftragten zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Absatz 1 Nummer 2 erfolgt sind. In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 80

Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 78 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 79 Absatz 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 78 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,
2. zur Wahrung berechtigter Interessen der betroffenen Person,
3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. im Einzelfall für die in § 45 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 45 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Absatz 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung über-wiegen.

(3) Für Übermittlungen nach Absatz 1 gilt § 79 Absatz 2 entsprechend.

§ 81

Sonstige Datenübermittlung an Empfänger in Drittstaaten

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 78 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,
2. die Übermittlung an die in § 78 Absatz 1 Nummer 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
3. der Verantwortliche dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

(2) Im Fall des Absatzes 1 hat der Verantwortliche die in § 78 Absatz 1 Nummer 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 79 Absatz 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Absatz 1 hat der Verantwortliche den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne seine Zustimmung nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

(5) Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

Kapitel 6

Zusammenarbeit der Aufsichtsbehörden

§ 82

Gegenseitige Amtshilfe

(1) Die oder der Bundesbeauftragte hat den Datenschutzaufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union Informationen zu übermitteln und Amtshilfe zu leisten, soweit dies für eine einheitliche Umsetzung und Anwendung der Richtlinie (EU) 2016/680 erforderlich ist. Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Die oder der Bundesbeauftragte hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen.

(3) Die oder der Bundesbeauftragte darf Amtshilfeersuchen nur ablehnen, wenn

1. sie oder er für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie oder er durchführen soll, nicht zuständig ist oder

2. ein Eingehen auf das Ersuchen gegen Rechtsvorschriften verstoßen würde.

(4) Die oder der Bundesbeauftragte hat die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. Sie oder er hat im Fall des Absatzes 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

(5) Die oder der Bundesbeauftragte hat die Informationen, um die sie oder er von der Aufsichtsbehörde des anderen Staates ersucht wurde, in der Regel elektronisch und in einem standardisierten Format zu übermitteln.

(6) Die oder der Bundesbeauftragte hat Amtshilfeersuchen kostenfrei zu erledigen, soweit sie

oder er nicht im Einzelfall mit der Aufsichtsbehörde des anderen Staates die Erstattung entstandener Ausgaben vereinbart hat.

(7) Ein Amtshilfeersuchen der oder des Bundesbeauftragten hat alle erforderlichen Informationen zu enthalten; hierzu gehören insbesondere der Zweck und die Begründung des Ersuchens. Die auf das Ersuchen übermittelten Informationen dürfen ausschließlich zu dem Zweck verwendet werden, zu dem sie angefordert wurden.

Kapitel 7

Haftung und Sanktionen

§ 83

Schadensersatz und Entschädigung

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise sein Rechtsträger.

(4) Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

(5) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

§ 84

Strafvorschriften

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 45 Satz 1, 3 oder 4 findet § 42 entsprechende Anwendung.

Teil 4

Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten

§ 85

Verarbeitung personenbezogener Daten im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten

(1) Die Übermittlung personenbezogener Daten an einen Drittstaat oder an über- oder zwischenstaatliche Stellen oder internationale Organisationen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten ist über die bereits gemäß der Verordnung (EU) 2016/679 zulässigen Fälle hinaus auch dann zulässig, wenn sie zur Erfüllung eigener Aufgaben aus zwingenden Gründen der Verteidigung oder zur Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist. Der Empfänger ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden.

(2) Für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten durch Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung gilt § 16 Absatz 4 nicht, soweit das Bundesministerium der Verteidigung im Einzelfall feststellt, dass die Erfüllung der dort genannten Pflichten die Sicherheit des Bundes gefährden würde.

(3) Für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten durch öffentliche Stellen des Bundes besteht keine Informationspflicht gemäß Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679, wenn

1. es sich um Fälle des § 32 Absatz 1 Nummer 1 bis 3 handelt oder
2. durch ihre Erfüllung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, und deswegen das Interesse der betroffenen Person an der Erteilung der Information zurücktreten muss.

Ist die betroffene Person in den Fällen des Satzes 1 nicht zu informieren, besteht auch kein Recht auf Auskunft. § 32 Absatz 2 und § 33 Absatz 2 finden keine Anwendung

Anhang 5

Dieses Dokument ist lediglich eine Dokumentationsquelle, für deren Richtigkeit die Organe der Gemeinschaft keine Gewähr übernehmen.

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002

über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) im ABl. L 201 vom 31. Juli 2002, S. 37, zuletzt geändert durch Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 (ABl. EG Nr. L 105 S. 54) und Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. EG Nr. L 337 S. 11)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION -
gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,
insbesondere auf Artikel 95,
auf Vorschlag der Kommission,
nach Stellungnahme des Wirtschafts- und Sozialausschusses,
nach Anhörung des Ausschusses der Regionen,
gemäß dem Verfahren des Artikels 251 des Vertrags,
in Erwägung nachstehender Gründe:

(1) 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(4) schreibt vor, dass die Mitgliedstaaten die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten und insbesondere ihr Recht auf Privatsphäre sicherstellen, um in der Gemeinschaft den freien Verkehr personenbezogener Daten zu gewährleisten.

(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die Charta der Grundrechte der Europäischen Union anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 jener Charta niedergelegten Rechte uneingeschränkt geachtet werden.

(3) Die Vertraulichkeit der Kommunikation wird nach den internationalen Menschenrechtsübereinkünften, insbesondere der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, und den Verfassungen der Mitgliedstaaten garantiert.

(4) Mit der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation(5) wurden die Grundsätze der Richtlinie 95/46/EG in spezielle Vorschriften für den Telekommunikationssektor umgesetzt. Die Richt-

linie 97/66/EG muss an die Entwicklungen der Märkte und Technologien für elektronische Kommunikationsdienste angepasst werden, um den Nutzern öffentlich zugänglicher elektronischer Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie den gleichen Grad des Schutzes personenbezogener Daten und der Privatsphäre zu bieten. Jene Richtlinie ist daher aufzuheben und durch die vorliegende Richtlinie zu ersetzen.

(5) Gegenwärtig werden öffentliche Kommunikationsnetze in der Gemeinschaft mit fortschrittlichen neuen Digitaltechnologien ausgestattet, die besondere Anforderungen an den Schutz personenbezogener Daten und der Privatsphäre des Nutzers mit sich bringen. Die Entwicklung der Informationsgesellschaft ist durch die Einführung neuer elektronischer Kommunikationsdienste gekennzeichnet. Der Zugang zu digitalen Mobilfunknetzen ist für breite Kreise möglich und erschwinglich geworden. Diese digitalen Netze verfügen über große Kapazitäten und Möglichkeiten zur Datenverarbeitung. Die erfolgreiche grenzüberschreitende Entwicklung dieser Dienste hängt zum Teil davon ab, inwieweit die Nutzer darauf vertrauen, dass ihre Privatsphäre unangetastet bleibt.

(6) Das Internet revolutioniert die herkömmlichen Marktstrukturen, indem es eine gemeinsame, weltweite Infrastruktur für die Bereitstellung eines breiten Spektrums elektronischer Kommunikationsdienste bietet. Öffentlich zugängliche elektronische Kommunikationsdienste über das Internet eröffnen neue Möglichkeiten für die Nutzer, bilden aber auch neue Risiken in Bezug auf ihre personenbezogenen Daten und ihre Privatsphäre.

(7) Für öffentliche Kommunikationsnetze sollten besondere rechtliche, ordnungspolitische und technische Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und der berechtigten Interessen juristischer Personen erlassen werden, insbesondere im Hinblick auf die zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung personenbezogener Daten über Teilnehmer und Nutzer.

(8) Die von den Mitgliedstaaten erlassenen rechtlichen, ordnungspolitischen und technischen Bestimmungen zum Schutz personenbezogener Daten, der Privatsphäre und der berechtigten Interessen juristischer Personen im Bereich der elektronischen Kommunikation sollten harmonisiert werden, um Behinderungen des Binnenmarktes der elektronischen Kommunikation nach Artikel 14 des Vertrags zu beseitigen. Die Harmonisierung sollte sich auf die Anforderungen beschränken, die notwendig sind, um zu gewährleisten, dass die Entstehung und die Weiterentwicklung neuer elektronischer Kommunikationsdienste und -netze zwischen Mitgliedstaaten nicht behindert werden.

(9) Die Mitgliedstaaten, die betroffenen Anbieter und Nutzer sowie die zuständigen Stellen der Gemeinschaft sollten bei der Einführung und Weiterentwicklung der entsprechenden Technologien zusammenarbeiten, soweit dies zur Anwendung der in dieser Richtlinie vorgesehenen Garantien erforderlich ist; als Ziele zu berücksichtigen sind dabei insbesondere die Beschränkung der Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß und die Verwendung anonymer oder pseudonymer Daten.

(10) Im Bereich der elektronischen Kommunikation gilt die Richtlinie 95/46/EG vor allem für alle Fragen des Schutzes der Grundrechte und Grundfreiheiten, die von der vorliegenden Richtlinie nicht spezifisch erfasst werden, einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen. Die Richtlinie 95/46/EG gilt für nicht öffentliche Kommunikationsdienste.

(11) Wie die Richtlinie 95/46/EG gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.

(12) Bei den Teilnehmern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann es sich um natürliche oder juristische Personen handeln. Diese Richtlinie zielt durch Ergänzung der Richtlinie 95/46/EG darauf ab, die Grundrechte natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, sowie die berechtigten Interessen juristischer Personen zu schützen. Aus dieser Richtlinie ergibt sich keine Verpflichtung der Mitgliedstaaten, die Richtlinie 95/46/EG auf den Schutz der berechtigten Interessen juristischer Personen auszudehnen, der im Rahmen der geltenden gemeinschaftlichen und einzelstaatlichen Rechtsvorschriften sichergestellt ist.

(13) Das Vertragsverhältnis zwischen einem Teilnehmer und einem Diensteanbieter kann zu einer regelmäßigen oder einmaligen Zahlung für den erbrachten oder zu erbringenden Dienst führen. Auch vorbezahlte Karten gelten als eine Form des Vertrags.

(14) Standortdaten können sich beziehen auf den Standort des Endgeräts des Nutzers nach geografischer Länge, Breite und Höhe, die Übertragungsrichtung, den Grad der Genauigkeit der Standortinformationen, die Identifizierung des Netzpunktes, an dem sich das End-

gerät zu einem bestimmten Zeitpunkt befindet, und den Zeitpunkt, zu dem die Standortinformationen erfasst wurden.

(15) Eine Nachricht kann alle Informationen über Namen, Nummern oder Adressen einschließen, die der Absender einer Nachricht oder der Nutzer einer Verbindung für die Zwecke der Übermittlung der Nachricht bereitstellt. Der Begriff "Verkehrsdaten" kann alle Formen einschließen, in die diese Informationen durch das Netz, über das die Nachricht übertragen wird, für die Zwecke der Übermittlung umgewandelt werden. Verkehrsdaten können sich unter anderem auf die Leitwege, die Dauer, den Zeitpunkt oder die Datenmenge einer Nachricht, das verwendete Protokoll, den Standort des Endgeräts des Absenders oder Empfängers, das Netz, von dem die Nachricht ausgeht bzw. an das es gesendet wird, oder den Beginn, das Ende oder die Dauer einer Verbindung beziehen. Sie können auch das Format betreffen, in dem die Nachricht über das Netz weitergeleitet wird.

(16) Eine Information, die als Teil eines Rundfunkdienstes über ein öffentliches Kommunikationsnetz weitergeleitet wird, ist für einen potenziell unbegrenzten Personenkreis bestimmt und stellt keine Nachricht im Sinne dieser Richtlinie dar. Kann jedoch ein einzelner Teilnehmer oder Nutzer, der eine derartige Information erhält, beispielsweise durch einen Videoabruf-Dienst identifiziert werden, so ist die weitergeleitete Information als Nachricht im Sinne dieser Richtlinie zu verstehen.

(17) Für die Zwecke dieser Richtlinie sollte die Einwilligung des Nutzers oder Teilnehmers unabhängig davon, ob es sich um eine natürliche oder eine juristische Person handelt, dieselbe Bedeutung haben wie der in der Richtlinie 95/46/EG definierte und dort weiter präzisierte Begriff "Einwilligung der betroffenen Person". Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website.

(18) Dienste mit Zusatznutzen können beispielsweise die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen umfassen.

(19) Die Anwendung bestimmter Anforderungen für die Anzeige des rufenden und angerufenen Anschlusses sowie für die Einschränkung dieser Anzeige und für die automatische Weiterschaltung zu Teilnehmeranschlüssen, die an analoge Vermittlungen angeschlossen sind, sollte in besonderen Fällen nicht zwingend vorgeschrieben werden, wenn sich die Anwendung als technisch nicht machbar erweist oder einen unangemessen hohen wirtschaftlichen Aufwand erfordert. Für die Beteiligten ist es wichtig, in solchen Fällen in Kenntnis gesetzt zu werden, und die Mitgliedstaaten müssen sie deshalb der Kommission anzeigen.

(20) Diensteanbieter sollen geeignete Maßnahmen ergreifen, um die Sicherheit ihrer Dienste, erforderlichenfalls zusammen mit dem Netzbetreiber, zu gewährleisten, und die Teil-

nehmer über alle besonderen Risiken der Verletzung der Netzsicherheit unterrichten. Solche Risiken können vor allem bei elektronischen Kommunikationsdiensten auftreten, die über ein offenes Netz wie das Internet oder den analogen Mobilfunk bereitgestellt werden. Der Diensteanbieter muss die Teilnehmer und Nutzer solcher Dienste unbedingt vollständig über die Sicherheitsrisiken aufklären, gegen die er selbst keine Abhilfe bieten kann. Diensteanbieter, die öffentlich zugängliche elektronische Kommunikationsdienste über das Internet anbieten, sollten die Nutzer und Teilnehmer über Maßnahmen zum Schutz ihrer zu übertragenden Nachrichten informieren, wie z. B. den Einsatz spezieller Software oder von Verschlüsselungstechniken. Die Anforderung, die Teilnehmer über besondere Sicherheitsrisiken aufzuklären, entbindet einen Diensteanbieter nicht von der Verpflichtung, auf eigene Kosten unverzüglich geeignete Maßnahmen zu treffen, um einem neuen, unvorhergesehenen Sicherheitsrisiko vorzubeugen und den normalen Sicherheitsstandard des Dienstes wiederherzustellen. Abgesehen von den nominellen Kosten, die dem Teilnehmer bei Erhalt oder Abruf der Information entstehen, beispielsweise durch das Laden einer elektronischen Post, sollte die Bereitstellung der Informationen über Sicherheitsrisiken für die Teilnehmer kostenfrei sein. Die Bewertung der Sicherheit erfolgt unter Berücksichtigung des Artikels 17 der Richtlinie 95/46/EG.

(21) Es sollten Maßnahmen getroffen werden, um den unerlaubten Zugang zu Nachrichten – und zwar sowohl zu ihrem Inhalt als auch zu mit ihnen verbundenen Daten – zu verhindern und so die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen elektronischen Kommunikationsdiensten erfolgenden Nachrichtenübertragung zu schützen. Nach dem Recht einiger Mitgliedstaaten ist nur der absichtliche unberechtigte Zugriff auf die Kommunikation untersagt.

(22) Mit dem Verbot der Speicherung von Nachrichten und zugehörigen Verkehrsdaten durch andere Personen als die Nutzer oder ohne deren Einwilligung soll die automatische, einstweilige und vorübergehende Speicherung dieser Informationen insoweit nicht untersagt werden, als diese Speicherung einzig und allein zum Zwecke der Durchführung der Übertragung in dem elektronischen Kommunikationsnetz erfolgt und als die Information nicht länger gespeichert wird, als dies für die Übertragung und zum Zwecke der Verkehrsabwicklung erforderlich ist, und die Vertraulichkeit der Nachrichten gewahrt bleibt. Wenn dies für eine effizientere Weiterleitung einer öffentlich zugänglichen Information an andere Empfänger des Dienstes auf ihr Ersuchen hin erforderlich ist, sollte diese Richtlinie dem nicht entgegenstehen, dass die Information länger gespeichert wird, sofern diese Information der Öffentlichkeit auf jeden Fall uneingeschränkt zugänglich wäre und Daten, die einzelne, die Information anfordernde Teilnehmer oder Nutzer betreffen, gelöscht würden.

(23) Die Vertraulichkeit von Nachrichten sollte auch im Rahmen einer rechtmäßigen Geschäftspraxis sichergestellt sein. Falls erforderlich und rechtlich zulässig, können Nachrichten zum Nachweis einer kommerziellen Transaktion aufgezeichnet werden. Diese Art der Ver-

arbeitung fällt unter die Richtlinie 95/46/EG. Die von der Nachricht betroffenen Personen sollten vorab von der Absicht der Aufzeichnung, ihrem Zweck und der Dauer ihrer Speicherung in Kenntnis gesetzt werden. Die aufgezeichnete Nachricht sollte so schnell wie möglich und auf jeden Fall spätestens mit Ablauf der Frist gelöscht werden, innerhalb deren die Transaktion rechtmäßig angefochten werden kann.

(24) Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen sind Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt. So genannte "Spyware", "Web-Bugs", "Hidden Identifiers" und ähnliche Instrumente können ohne das Wissen des Nutzers in dessen Endgerät eindringen, um Zugang zu Informationen zu erlangen, oder die Nutzeraktivität zurückzuverfolgen und können eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen. Die Verwendung solcher Instrumente sollte nur für rechtmäßige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein.

(25) Solche Instrumente, z. B. so genannte "Cookies", können ein legitimes und nützliches Hilfsmittel sein, um die Wirksamkeit von Website-Gestaltung und Werbung zu untersuchen und die Identität der an Online-Transaktionen beteiligten Nutzer zu überprüfen. Dienen solche Instrumente, z. B. "Cookies", einem rechtmäßigen Zweck, z. B. der Erleichterung der Bereitstellung von Diensten der Informationsgesellschaft, so sollte deren Einsatz unter der Bedingung zugelassen werden, dass die Nutzer gemäß der Richtlinie 95/46/EG klare und genaue Informationen über den Zweck von Cookies oder ähnlichen Instrumenten erhalten, d. h., der Nutzer muss wissen, dass bestimmte Informationen auf dem von ihm benutzten Endgerät platziert werden. Die Nutzer sollten die Gelegenheit haben, die Speicherung eines Cookies oder eines ähnlichen Instruments in ihrem Endgerät abzulehnen. Dies ist besonders bedeutsam, wenn auch andere Nutzer Zugang zu dem betreffenden Endgerät haben und damit auch zu dort gespeicherten Daten, die sensible Informationen privater Natur beinhalten. Die Auskunft und das Ablehnungsrecht können einmalig für die Nutzung verschiedener in dem Endgerät des Nutzers während derselben Verbindung zu installierender Instrumente angeboten werden und auch die künftige Verwendung derartiger Instrumente umfassen, die während nachfolgender Verbindungen vorgenommen werden können. Die Modalitäten für die Erteilung der Informationen oder für den Hinweis auf das Verweigerungsrecht und die Einholung der Zustimmung sollten so benutzerfreundlich wie möglich sein. Der Zugriff auf spezifische Website-Inhalte kann nach wie vor davon abhängig gemacht werden, dass ein Cookie oder ein ähnliches Instrument von einer in Kenntnis der Sachlage gegebenen Einwilligung abhängig gemacht wird, wenn der Einsatz zu einem rechtmäßigen Zweck erfolgt.

(26) Teilnehmerdaten, die in elektronischen Kommunikationsnetzen zum Verbindungsaufbau und zur Nachrichtenübertragung verarbeitet werden, enthalten Informationen

über das Privatleben natürlicher Personen und betreffen ihr Recht auf Achtung ihrer Kommunikationsfreiheit, oder sie betreffen berechtigte Interessen juristischer Personen. Diese Daten dürfen nur für einen begrenzten Zeitraum und nur insoweit gespeichert werden, wie dies für die Erbringung des Dienstes, für die Gebührenabrechnung und für Zusammenschaltungszahlungen erforderlich ist. Jede weitere Verarbeitung solcher Daten, die der Betreiber des öffentlich zugänglichen elektronischen Kommunikationsdienstes zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen vornehmen möchte, darf nur unter der Bedingung gestattet werden, dass der Teilnehmer dieser Verarbeitung auf der Grundlage genauer, vollständiger Angaben des Betreibers des öffentlich zugänglichen elektronischen Kommunikationsdienstes über die Formen der von ihm beabsichtigten weiteren Verarbeitung und über das Recht des Teilnehmers, seine Einwilligung zu dieser Verarbeitung nicht zu erteilen oder zurückzuziehen, zugestimmt hat. Verkehrsdaten, die für die Vermarktung von Kommunikationsdiensten oder für die Bereitstellung von Diensten mit Zusatznutzen verwendet wurden, sollten ferner nach der Bereitstellung des Dienstes gelöscht oder anonymisiert werden. Diensteanbieter sollen die Teilnehmer stets darüber auf dem Laufenden halten, welche Art von Daten sie verarbeiten und für welche Zwecke und wie lange das geschieht.

(27) Der genaue Zeitpunkt des Abschlusses der Übermittlung einer Nachricht, nach dem die Verkehrsdaten außer zu Fakturierungszwecken gelöscht werden sollten, kann von der Art des bereitgestellten elektronischen Kommunikationsdienstes abhängen. Bei einem Sprach-Telefonanruf beispielsweise ist die Übermittlung abgeschlossen, sobald einer der Teilnehmer die Verbindung beendet. Bei der elektronischen Post ist die Übermittlung dann abgeschlossen, wenn der Adressat die Nachricht – üblicherweise vom Server seines Diensteanbieters – abruft.

(28) Die Verpflichtung, Verkehrsdaten zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, steht nicht im Widerspruch zu im Internet angewandten Verfahren wie dem Caching von IP-Adressen im Domain-Namen-System oder dem Caching einer IP-Adresse, die einer physischen Adresse zugeordnet ist, oder der Verwendung von Informationen über den Nutzer zum Zwecke der Kontrolle des Rechts auf Zugang zu Netzen oder Diensten.

(29) Der Diensteanbieter kann Verkehrsdaten in Bezug auf Teilnehmer und Nutzer in Einzelfällen verarbeiten, um technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln. Für Fakturierungszwecke notwendige Verkehrsdaten dürfen ebenfalls vom Diensteanbieter verarbeitet werden, um Fälle von Betrug, die darin bestehen, die elektronischen Kommunikationsdienste ohne entsprechende Bezahlung nutzen, ermitteln und abstellen zu können.

(30) Die Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste soll-

ten so konzipiert werden, dass so wenig personenbezogene Daten wie möglich benötigt werden. Jedwede Tätigkeit im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste, die über die Übermittlung einer Nachricht und die Fakturierung dieses Vorgangs hinausgeht, sollte auf aggregierten Verkehrsdaten basieren, die nicht mit Teilnehmern oder Nutzern in Verbindung gebracht werden können. Können diese Tätigkeiten nicht auf aggregierte Daten gestützt werden, so sollten sie als Dienste mit Zusatznutzen angesehen werden, für die die Einwilligung des Teilnehmers erforderlich ist.

(31) Ob die Einwilligung in die Verarbeitung personenbezogener Daten im Hinblick auf die Erbringung eines speziellen Dienstes mit Zusatznutzen beim Nutzer oder beim Teilnehmer eingeholt werden muss, hängt von den zu verarbeitenden Daten, von der Art des zu erbringenden Dienstes und von der Frage ab, ob es technisch, verfahrenstechnisch und vertraglich möglich ist, zwischen der einen elektronischen Kommunikationsdienst in Anspruch nehmenden Einzelperson und der an diesem Dienst teilnehmenden juristischen oder natürlichen Person zu unterscheiden.

(32) Vergibt der Betreiber eines elektronischen Kommunikationsdienstes oder eines Dienstes mit Zusatznutzen die für die Bereitstellung dieser Dienste erforderliche Verarbeitung personenbezogener Daten an eine andere Stelle weiter, so sollten diese Weitervergabe und die anschließende Datenverarbeitung in vollem Umfang den Anforderungen in Bezug auf die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter im Sinne der Richtlinie 95/46/EG entsprechen. Erfordert die Bereitstellung eines Dienstes mit Zusatznutzen die Weitergabe von Verkehrsdaten oder Standortdaten von dem Betreiber eines elektronischen Kommunikationsdienstes an einen Betreiber eines Dienstes mit Zusatznutzen, so sollten die Teilnehmer oder Nutzer, auf die sich die Daten beziehen, ebenfalls in vollem Umfang über diese Weitergabe unterrichtet werden, bevor sie in die Verarbeitung der Daten einwilligen.

(33) Durch die Einführung des Einzelgebührennachweises hat der Teilnehmer mehr Möglichkeiten erhalten, die Richtigkeit der vom Diensteanbieter erhobenen Entgelte zu überprüfen, gleichzeitig kann dadurch aber eine Gefahr für die Privatsphäre der Nutzer öffentlich zugänglicher elektronischer Kommunikationsdienste entstehen. Um die Privatsphäre des Nutzers zu schützen, müssen die Mitgliedstaaten daher darauf hinwirken, dass bei den elektronischen Kommunikationsdiensten beispielsweise alternative Funktionen entwickelt werden, die den anonymen oder rein privaten Zugang zu öffentlich zugänglichen elektronischen Kommunikationsdiensten ermöglichen, beispielsweise Telefonkarten und Möglichkeiten der Zahlung per Kreditkarte. Zu dem gleichen Zweck können die Mitgliedstaaten die Anbieter auffordern, ihren Teilnehmern eine andere Art von ausführlicher Rechnung anzubieten, in der eine bestimmte Anzahl von Ziffern der Rufnummer unkenntlich gemacht ist.

(34) Im Hinblick auf die Rufnummernanzeige ist es erforderlich, das Recht des Anrufers zu wahren, die Anzeige der Rufnummer des Anschlusses, von dem aus der Anruf erfolgt, zu

unterdrücken, ebenso wie das Recht des Angerufenen, Anrufe von nicht identifizierten Anschlüssen abzuweisen. Es ist gerechtfertigt, in Sonderfällen die Unterdrückung der Rufnummernanzeige aufzuheben. Bestimmte Teilnehmer, insbesondere telefonische Beratungsdienste und ähnliche Einrichtungen, haben ein Interesse daran, die Anonymität ihrer Anrufer zu gewährleisten. Im Hinblick auf die Anzeige der Rufnummer des Angerufenen ist es erforderlich, das Recht und das berechtigte Interesse des Angerufenen zu wahren, die Anzeige der Rufnummer des Anschlusses, mit dem der Anrufer tatsächlich verbunden ist, zu unterdrücken; dies gilt besonders für den Fall weitergeschalteter Anrufe. Die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste sollten ihre Teilnehmer über die Möglichkeit der Anzeige der Rufnummer des Anrufenden und des Angerufenen, über alle Dienste, die auf der Grundlage der Anzeige der Rufnummer des Anrufenden und des Angerufenen angeboten werden, sowie über die verfügbaren Funktionen zur Wahrung der Vertraulichkeit unterrichten. Die Teilnehmer können dann sachkundig die Funktionen auswählen, die sie zur Wahrung der Vertraulichkeit nutzen möchten. Die Funktionen zur Wahrung der Vertraulichkeit, die anschlussbezogen angeboten werden, müssen nicht unbedingt als automatischer Netzdienst zur Verfügung stehen, sondern können von dem Betreiber des öffentlich zugänglichen elektronischen Kommunikationsdienstes auf einfachen Antrag bereitgestellt werden.

(35) In digitalen Mobilfunknetzen werden Standortdaten verarbeitet, die Aufschluss über den geografischen Standort des Endgeräts des mobilen Nutzers geben, um die Nachrichtenübertragung zu ermöglichen. Solche Daten sind Verkehrsdaten, die unter Artikel 6 dieser Richtlinie fallen. Doch können digitale Mobilfunknetze zusätzlich auch in der Lage sein, Standortdaten zu verarbeiten, die genauer sind als es für die Nachrichtenübertragung erforderlich wäre und die für die Bereitstellung von Diensten mit Zusatznutzen verwendet werden, wie z. B. persönliche Verkehrsinformationen und Hilfen für den Fahrzeugführer. Die Verarbeitung solcher Daten für die Bereitstellung von Diensten mit Zusatznutzen soll nur dann gestattet werden, wenn die Teilnehmer darin eingewilligt haben. Selbst dann sollten sie die Möglichkeit haben, die Verarbeitung von Standortdaten auf einfache Weise und gebührenfrei zeitweise zu untersagen.

(36) Die Mitgliedstaaten können die Rechte der Nutzer und Teilnehmer auf Privatsphäre in Bezug auf die Rufnummernanzeige einschränken, wenn dies erforderlich ist, um belästigende Anrufe zurückzuverfolgen; in Bezug auf Rufnummernanzeige und Standortdaten kann dies geschehen, wenn es erforderlich ist, Notfalldiensten zu ermöglichen, ihre Aufgaben so effektiv wie möglich zu erfuellen. Hierzu können die Mitgliedstaaten besondere Vorschriften erlassen, um die Anbieter von elektronischen Kommunikationsdiensten zu ermächtigen, einen Zugang zur Rufnummernanzeige und zu Standortdaten ohne vorherige Einwilligung der betreffenden Nutzer oder Teilnehmer zu verschaffen.

(37) Es sollten Vorkehrungen getroffen werden, um die Teilnehmer vor eventueller Belästigung

durch die automatische Weiterschaltung von Anrufen durch andere zu schützen. In derartigen Fällen muss der Teilnehmer durch einfachen Antrag beim Betreiber des öffentlich zugänglichen elektronischen Kommunikationsdienstes die Weiterschaltung von Anrufen auf sein Endgerät unterbinden können.

(38) Die Verzeichnisse der Teilnehmer elektronischer Kommunikationsdienste sind weit verbreitet und öffentlich. Das Recht auf Privatsphäre natürlicher Personen und das berechtigte Interesse juristischer Personen erfordern daher, dass die Teilnehmer bestimmen können, ob ihre persönlichen Daten – und gegebenenfalls welche – in einem Teilnehmerverzeichnis veröffentlicht werden. Die Anbieter öffentlicher Verzeichnisse sollten die darin aufzunehmenden Teilnehmer über die Zwecke des Verzeichnisses und eine eventuelle besondere Nutzung elektronischer Fassungen solcher Verzeichnisse informieren; dabei ist insbesondere an in die Software eingebettete Suchfunktionen gedacht, etwa die umgekehrte Suche, mit deren Hilfe Nutzer des Verzeichnisses den Namen und die Anschrift eines Teilnehmers allein aufgrund dessen Telefonnummer herausfinden können.

(39) Die Verpflichtung zur Unterrichtung der Teilnehmer über den Zweck bzw. die Zwecke öffentlicher Verzeichnisse, in die ihre personenbezogenen Daten aufzunehmen sind, sollte demjenigen auferlegt werden, der die Daten für die Aufnahme erhebt. Können die Daten an einen oder mehrere Dritte weitergegeben werden, so sollte der Teilnehmer über diese Möglichkeit und über den Empfänger oder die Kategorien möglicher Empfänger unterrichtet werden. Voraussetzung für die Weitergabe sollte sein, dass die Daten nicht für andere Zwecke als diejenigen verwendet werden, für die sie erhoben wurden. Wünscht derjenige, der die Daten beim Teilnehmer erhebt, oder ein Dritter, an den die Daten weitergegeben wurden, diese Daten zu einem weiteren Zweck zu verwenden, so muss entweder der ursprüngliche Datenerheber oder der Dritte, an den die Daten weitergegeben wurden, die erneute Einwilligung des Teilnehmers einholen.

(40) Es sollten Vorkehrungen getroffen werden, um die Teilnehmer gegen die Verletzung ihrer Privatsphäre durch unerbetene Nachrichten für Zwecke der Direktwerbung, insbesondere durch automatische Anrufsysteme, Faxgeräte und elektronische Post, einschließlich SMS, zu schützen. Diese Formen von unerbetenen Werbenachrichten können zum einen relativ leicht und preiswert zu versenden sein und zum anderen eine Belastung und/oder einen Kostenaufwand für den Empfänger bedeuten. Darüber hinaus kann in einigen Fällen ihr Umfang auch Schwierigkeiten für die elektronischen Kommunikationsnetze und die Endgeräte verursachen. Bei solchen Formen unerbetener Nachrichten zum Zweck der Direktwerbung ist es gerechtfertigt, zu verlangen, die Einwilligung der Empfänger einzuholen, bevor ihnen solche Nachrichten gesandt werden. Der Binnenmarkt verlangt einen harmonisierten Ansatz, damit für die Unternehmen und die Nutzer einfache, gemeinschaftsweite Regeln gelten.

(41) Im Rahmen einer bestehenden Kundenbeziehung ist es vertretbar, die Nutzung elektronischer Kontaktinformationen zuzulassen, damit ähnliche Produkte oder Dienstleistungen angeboten werden; dies gilt jedoch nur für dasselbe Unternehmen, das auch die Kontaktinformationen gemäß der Richtlinie 95/46/EG erhalten hat. Bei der Erlangung der Kontaktinformationen sollte der Kunde über deren weitere Nutzung zum Zweck der Direktwerbung klar und eindeutig unterrichtet werden und die Möglichkeit erhalten, diese Verwendung abzulehnen. Diese Möglichkeit sollte ferner mit jeder weiteren als Direktwerbung gesendeten Nachricht gebührenfrei angeboten werden, wobei Kosten für die Übermittlung der Ablehnung nicht unter die Gebührenfreiheit fallen.

(42) Sonstige Formen der Direktwerbung, die für den Absender kostspieliger sind und für die Teilnehmer und Nutzer keine finanziellen Kosten mit sich bringen, wie Sprach-Telefonanrufe zwischen Einzelpersonen, können die Beibehaltung eines Systems rechtfertigen, bei dem die Teilnehmer oder Nutzer die Möglichkeit erhalten, zu erklären, dass sie solche Anrufe nicht erhalten möchten. Damit das bestehende Niveau des Schutzes der Privatsphäre nicht gesenkt wird, sollten die Mitgliedstaaten jedoch einzelstaatliche Systeme beibehalten können, bei denen solche an Teilnehmer und Nutzer gerichtete Anrufe nur gestattet werden, wenn diese vorher ihre Einwilligung gegeben haben.

(43) Zur Erleichterung der wirksamen Durchsetzung der Gemeinschaftsvorschriften für unerbetene Nachrichten zum Zweck der Direktwerbung ist es notwendig, die Verwendung falscher Identitäten oder falscher Absenderadressen oder Anrufernummern beim Versand unerbetener Nachrichten zum Zweck der Direktwerbung zu untersagen.

(44) Bei einigen elektronischen Postsystemen können die Teilnehmer Absender und Betreffzeile einer elektronischen Post sehen und darüber hinaus diese Post löschen, ohne die gesamte Post oder deren Anlagen herunterladen zu müssen; dadurch lassen sich die Kosten senken, die möglicherweise mit dem Herunterladen unerwünschter elektronischer Post oder deren Anlagen verbunden sind. Diese Verfahren können in bestimmten Fällen zusätzlich zu den in dieser Richtlinie festgelegten allgemeinen Verpflichtungen von Nutzen bleiben.

(45) Diese Richtlinie berührt nicht die Vorkehrungen der Mitgliedstaaten, mit denen die legitimen Interessen juristischer Personen gegen unerbetene Direktwerbungsnachrichten geschützt werden sollen. Errichten die Mitgliedstaaten ein Register der juristischen Personen – großenteils gewerbetreibende Nutzer -, die derartige Nachrichten nicht erhalten möchten (“opt-out Register”), so gilt Artikel 7 der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (“Richtlinie über den elektronischen Geschäftsverkehr”)(6) in vollem Umfang.

(46) Die Funktion für die Bereitstellung elektronischer Kommunikationsdienste kann in das Netz oder in irgendeinen Teil des Endgeräts des Nutzers, auch in die Software, eingebaut

sein. Der Schutz personenbezogener Daten und der Privatsphäre des Nutzers öffentlich zugänglicher elektronischer Kommunikationsdienste sollte nicht von der Konfiguration der für die Bereitstellung des Dienstes notwendigen Komponenten oder von der Verteilung der erforderlichen Funktionen auf diese Komponenten abhängen. Die Richtlinie 95/46/EG gilt unabhängig von der verwendeten Technologie für alle Formen der Verarbeitung personenbezogener Daten. Bestehen neben allgemeinen Vorschriften für die Komponenten, die für die Bereitstellung elektronischer Kommunikationsdienste notwendig sind, auch noch spezielle Vorschriften für solche Dienste, dann erleichtert dies nicht unbedingt den technologieunabhängigen Schutz personenbezogener Daten und der Privatsphäre. Daher könnten sich Maßnahmen als notwendig erweisen, mit denen die Hersteller bestimmter Arten von Geräten, die für elektronische Kommunikationsdienste benutzt werden, verpflichtet werden, in ihren Produkten von vornherein Sicherheitsfunktionen vorzusehen, die den Schutz personenbezogener Daten und der Privatsphäre des Nutzers und Teilnehmers gewährleisten. Der Erlass solcher Maßnahmen in Einklang mit der Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität(7) gewährleistet, dass die aus Gründen des Datenschutzes erforderliche Einführung von technischen Merkmalen elektronischer Kommunikationsgeräte einschließlich der Software harmonisiert wird, damit sie der Verwirklichung des Binnenmarktes nicht entgegensteht.

(47) Das innerstaatliche Recht sollte Rechtsbehelfe für den Fall vorsehen, dass die Rechte der Benutzer und Teilnehmer nicht respektiert werden. Gegen jede – privatem oder öffentlichem Recht unterliegende – Person, die den nach dieser Richtlinie getroffenen einzelstaatlichen Maßnahmen zuwiderhandelt, sollten Sanktionen verhängt werden.

(48) Bei der Anwendung dieser Richtlinie ist es sinnvoll, auf die Erfahrung der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Datenschutzgruppe aus Vertretern der für den Schutz personenbezogener Daten zuständigen Kontrollstellen der Mitgliedstaaten zurückzugreifen.

(49) Zur leichteren Einhaltung der Vorschriften dieser Richtlinie bedarf es einer Sonderregelung für die Datenverarbeitungen, die zum Zeitpunkt des Inkrafttretens der nach dieser Richtlinie erlassenen innerstaatlichen Vorschriften bereits durchgeführt werden -

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1
Geltungsbereich und Zielsetzung

(1) Diese Richtlinie dient der Harmonisierung der Vorschriften der Mitgliedstaaten, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener

Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.

Artikel 2
Begriffsbestimmungen

Sofern nicht anders angegeben, gelten die Begriffsbestimmungen der Richtlinie 95/46/EG und der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste („Rahmenrichtlinie") (8) auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

a) „Nutzer" eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

b) „Verkehrsdaten" Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

c) „Standortdaten" Daten, die in einem elektronischen Kommunikationsnetz verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

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

e) „Anruf" eine über einen öffentlich zugänglichen Telefondienst aufgebaute Verbindung, die eine zweiseitige Echtzeit-Kommunikation ermöglicht;

f) „Einwilligung" eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG;

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

h) „elektronische Post" jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.

Artikel 3
Betroffene Dienste

(1) Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft.

(2) Die Artikel 8, 10 und 11 gelten für Teilnehmeranschlüsse, die an digitale Vermittlungsstellen angeschlossen sind, und – soweit dies technisch machbar ist und keinen unverhältnismäßigen wirtschaftlichen Aufwand erfordert – für Teilnehmeranschlüsse, die an analoge Vermittlungsstellen angeschlossen sind.

(3) Die Mitgliedstaaten teilen der Kommission die Fälle mit, in denen eine Einhaltung der Anforderungen der Artikel 8, 10 und 11 technisch nicht machbar wäre oder einen unverhältnismäßigen wirtschaftlichen Aufwand erfordern würde.

Artikel 4
Betriebssicherheit

(1) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

(2) Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes die Teilnehmer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten.

Artikel 5
Vertraulichkeit der Kommunikation

(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.

(2) Absatz 1 betrifft nicht das rechtlich zulässige Aufzeichnen von Nachrichten und der damit verbundenen Verkehrsdaten, wenn dies im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis einer kommerziellen Transaktion oder einer sonstigen geschäftlichen Nachricht geschieht.

(3) Die Mitgliedstaaten stellen sicher, dass die Benutzung elektronischer Kommunikationsnetze für die Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur unter der Bedingung gestattet ist, dass der betreffende Teilnehmer oder Nutzer gemäß der Richtlinie 95/46/EG klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhält und durch den für diese Verarbeitung Verantwortlichen auf das Recht hingewiesen wird, diese Verarbeitung zu verweigern. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen.

Artikel 6
Verkehrsdaten

(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.

(2) Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, dürfen verarbeitet werden. Diese Verarbeitung ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz 1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, seine Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zurückzuziehen.

(4) Der Diensteanbieter muss dem Teilnehmer oder Nutzer mitteilen, welche Arten von Verkehrsdaten für die in Absatz 2 genannten Zwecke verarbeitet werden und wie lange das geschieht; bei einer Verarbeitung für die in Absatz 3 genannten Zwecke muss diese Mitteilung erfolgen, bevor um Einwilligung ersucht wird.

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.

(6) Die Absätze 1, 2, 3 und 5 gelten unbeschadet der Möglichkeit der zuständigen Gremien, in Einklang mit den geltenden Rechtsvorschriften für die Beilegung von Streitigkeiten, insbesondere Zusammenschaltungs- oder Abrechnungsstreitigkeiten, von Verkehrsdaten Kenntnis zu erhalten.

Artikel 7
Einzelgebührennachweis

(1) Die Teilnehmer haben das Recht, Rechnungen ohne Einzelgebührennachweis zu erhalten.

(2) Die Mitgliedstaaten wenden innerstaatliche Vorschriften an, um das Recht der Teilnehmer, Einzelgebührennachweise zu erhalten, und das Recht anrufender Nutzer und angerufener Teilnehmer auf Vertraulichkeit miteinander in Einklang zu bringen, indem sie beispielsweise sicherstellen, dass diesen Nutzern und Teilnehmern genügend andere, den Schutz der Privatsphäre fördernde Methoden für die Kommunikation oder Zahlungen zur Verfügung stehen.

Artikel 8
Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung

(1) Wird die Anzeige der Rufnummer des Anrufers angeboten, so muss der Diensteanbieter dem anrufenden Nutzer die Möglichkeit geben, die Rufnummernanzeige für jeden Anruf einzeln auf einfache Weise und gebührenfrei zu verhindern. Dem anrufenden Teilnehmer muss diese Möglichkeit anschlussbezogen zur Verfügung stehen.

(2) Wird die Anzeige der Rufnummer des Anrufers angeboten, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, die Anzeige der Rufnummer eingehender Anrufe auf einfache Weise und für jede vertretbare Nutzung dieser Funktion gebührenfrei zu verhindern.

(3) Wird die Anzeige der Rufnummer des Anrufers angeboten und wird die Rufnummer vor der Herstellung der Verbindung angezeigt, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, eingehende Anrufe, bei denen die Rufnummernanzeige durch den anrufenden Nutzer oder Teilnehmer verhindert wurde, auf einfache Weise und gebührenfrei abzuweisen.

(4) Wird die Anzeige der Rufnummer des Angerufenen angeboten, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, die Anzeige seiner Rufnummer beim anrufenden Nutzer auf einfache Weise und gebührenfrei zu verhindern.

(5) Absatz 1 gilt auch für aus der Gemeinschaft kommende Anrufe in Drittländern. Die Absätze 2, 3 und 4 gelten auch für aus Drittländern kommende Anrufe.

(6) Wird die Anzeige der Rufnummer des Anrufers und/oder des Angerufenen angeboten, so stellen die Mitgliedstaaten sicher, dass die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste die Öffentlichkeit hierüber und über die in den Absätzen 1, 2, 3 und 4 beschriebenen Möglichkeiten unterrichten.

Artikel 9
Andere Standortdaten als Verkehrsdaten

(1) Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. Die Nutzer oder Teilnehmer können ihre Einwilligung zur Verarbeitung anderer Standortdaten als Verkehrsdaten jederzeit zurückziehen.

(2) Haben die Nutzer oder Teilnehmer ihre Einwilligung zur Verarbeitung von anderen Standortdaten als Verkehrsdaten gegeben, dann müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Kommunikationsnetzes oder öffentlich zugänglichen Kommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

Artikel 10
Ausnahmen

Die Mitgliedstaaten stellen sicher, dass es transparente Verfahren gibt, nach denen der Betreiber eines öffentlichen Kommunikationsnetzes und/oder eines öffentlich zugänglichen elektronischen Kommunikationsdienstes

a) die Unterdrückung der Anzeige der Rufnummer des Anrufers vorübergehend aufheben kann, wenn ein Teilnehmer beantragt hat, dass böswillige oder belästigende Anrufe zurückverfolgt werden; in diesem Fall werden nach innerstaatlichem Recht die Daten mit der Rufnummer des anrufenden Teilnehmers vom Betreiber des öffentlichen Kommunikationsnetzes und/oder des öffentlich zugänglichen elektronischen Kommunikationsdienstes gespeichert und zur Verfügung gestellt;

b) die Unterdrückung der Anzeige der Rufnummer des Anrufers aufheben und Standortdaten trotz der vorübergehenden Untersagung oder fehlenden Einwilligung durch den

Teilnehmer oder Nutzer verarbeiten kann, und zwar anschlussbezogen für Einrichtungen, die Notrufe bearbeiten und dafür von einem Mitgliedstaat anerkannt sind, einschließlich Strafverfolgungsbehörden, Ambulanzdiensten und Feuerwehren, zum Zwecke der Beantwortung dieser Anrufe.

Artikel 11
Automatische Anrufweiterschaltung

Die Mitgliedstaaten stellen sicher, dass jeder Teilnehmer die Möglichkeit hat, auf einfache Weise und gebührenfrei die von einer dritten Partei veranlasste automatische Anrufweiterschaltung zum Endgerät des Teilnehmers abzustellen.

Artikel 12
Teilnehmerverzeichnisse

(1) Die Mitgliedstaaten stellen sicher, dass die Teilnehmer gebührenfrei und vor Aufnahme in das Teilnehmerverzeichnis über den Zweck bzw. die Zwecke von gedruckten oder elektronischen, der Öffentlichkeit unmittelbar oder über Auskunftsdienste zugänglichen Teilnehmerverzeichnissen, in die ihre personenbezogenen Daten aufgenommen werden können, sowie über weitere Nutzungsmöglichkeiten aufgrund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen informiert werden.

(2) Die Mitgliedstaaten stellen sicher, dass die Teilnehmer Gelegenheit erhalten festzulegen, ob ihre personenbezogenen Daten – und ggf. welche – in ein öffentliches Verzeichnis aufgenommen werden, sofern diese Daten für den vom Anbieter des Verzeichnisses angegebenen Zweck relevant sind, und diese Daten prüfen, korrigieren oder löschen dürfen. Für die Nicht-Aufnahme in ein der Öffentlichkeit zugängliches Teilnehmerverzeichnis oder die Prüfung, Berichtigung oder Streichung personenbezogener Daten aus einem solchen Verzeichnis werden keine Gebühren erhoben.

(3) Die Mitgliedstaaten können verlangen, dass eine zusätzliche Einwilligung der Teilnehmer eingeholt wird, wenn ein öffentliches Verzeichnis anderen Zwecken als der Suche nach Einzelheiten betreffend die Kommunikation mit Personen anhand ihres Namens und gegebenenfalls eines Mindestbestands an anderen Kennzeichen dient.

(4) Die Absätze 1 und 2 gelten für Teilnehmer, die natürliche Personen sind. Die Mitgliedstaaten tragen im Rahmen des Gemeinschaftsrechts und der geltenden einzelstaatlichen Rechtsvorschriften außerdem dafür Sorge, dass die berechtigten Interessen anderer Teilnehmer als natürlicher Personen in Bezug auf ihre Aufnahme in öffentliche Verzeichnisse ausreichend geschützt werden.

Artikel 13
Unerbetene Nachrichten

(1) Die Verwendung von automatischen Anrufsystemen ohne menschlichen Eingriff (automatische Anrufmaschinen), Faxgeräten oder elektronischer Post für die Zwecke der Direktwerbung darf nur bei vorheriger Einwilligung der Teilnehmer gestattet werden.

(2) Ungeachtet des Absatzes 1 kann eine natürliche oder juristische Person, wenn sie von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung gemäß der Richtlinie 95/46/EG deren elektronische Kontaktinformationen für elektronische Post erhalten hat, diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden, sofern die Kunden klar und deutlich die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen, wenn der Kunde diese Nutzung nicht von vornherein abgelehnt hat.

(3) Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um – gebührenfrei für die Teilnehmer – sicherzustellen, dass außer in den in den Absätzen 1 und 2 genannten Fällen unerbetene Nachrichten zum Zweck der Direktwerbung, die entweder ohne die Einwilligung der betreffenden Teilnehmer erfolgen oder an Teilnehmer gerichtet sind, die keine solchen Nachrichten erhalten möchten, nicht gestattet sind; welche dieser Optionen gewählt wird, ist im innerstaatlichen Recht zu regeln.

(4) Auf jeden Fall verboten ist die Praxis des Versendens elektronischer Nachrichten zu Zwecken der Direktwerbung, bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

(5) Die Absätze 1 und 3 gelten für Teilnehmer, die natürliche Personen sind. Die Mitgliedstaaten tragen im Rahmen des Gemeinschaftsrechts und der geltenden einzelstaatlichen Rechtsvorschriften außerdem dafür Sorge, dass die berechtigten Interessen anderer Teilnehmer als natürlicher Personen in Bezug auf unerbetene Nachrichten ausreichend geschützt werden.

Artikel 14
Technische Merkmale und Normung

(1) Bei der Durchführung der Bestimmungen dieser Richtlinie stellen die Mitgliedstaaten vorbehaltlich der Absätze 2 und 3 sicher, dass keine zwingenden Anforderungen in Bezug auf spezifische technische Merkmale für Endgeräte oder sonstige elektronische Kommunikationsgeräte gestellt werden, die deren Inverkehrbringen und freien Vertrieb in und zwischen den Mitgliedstaaten behindern können.

(2) Soweit die Bestimmungen dieser Richtlinie nur mit Hilfe spezifischer technischer Merkmale elektronischer Kommunikationsnetze durchgeführt werden können, unterrichten die Mitgliedstaaten die Kommission darüber gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft(9).

(3) Erforderlichenfalls können gemäß der Richtlinie 1999/5/EG und dem Beschluss 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation(10) Maßnahmen getroffen werden, um sicherzustellen, dass Endgeräte in einer Weise gebaut sind, die mit dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist.

Artikel 15
Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

(2) Die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

(3) Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr.

Artikel 16
Übergangsbestimmungen

(1) Artikel 12 gilt nicht für Ausgaben von Teilnehmerverzeichnissen, die vor dem Inkrafttreten der nach dieser Richtlinie erlassenen innerstaatlichen Vorschriften bereits in gedruckter oder in netzunabhängiger elektronischer Form produziert oder in Verkehr gebracht wurden.

(2) Sind die personenbezogenen Daten von Teilnehmern von Festnetz- oder Mobil-Sprachtelefondiensten in ein öffentliches Teilnehmerverzeichnis gemäß der Richtlinie 95/46/EG und gemäß Artikel 11 der Richtlinie 97/66/EG aufgenommen worden, bevor die nach der vorliegenden Richtlinie erlassenen innerstaatlichen Rechtsvorschriften in Kraft treten, so können die personenbezogenen Daten dieser Teilnehmer in der gedruckten oder elektronischen Fassung, einschließlich Fassungen mit Umkehrsuchfunktionen, in diesem öffentlichen Verzeichnis verbleiben, sofern die Teilnehmer nach Erhalt vollständiger Informationen über die Zwecke und Möglichkeiten gemäß Artikel 12 nicht etwas anderes wünschen.

Artikel 17
Umsetzung

(1) Die Mitgliedstaaten setzen vor dem 31. Oktober 2003 die Rechtsvorschriften in Kraft, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der innerstaatlichen Rechts-Vorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen, sowie aller späteren Änderungen dieser Vorschriften.

Artikel 18
Überprüfung

Die Kommission unterbreitet dem Europäischen Parlament und dem Rat spätestens drei Jahre nach dem in Artikel 17 Absatz 1 genannten Zeitpunkt einen Bericht über die Durchführung dieser Richtlinie und ihre Auswirkungen auf die Wirtschaftsteilnehmer und Verbraucher, insbesondere in Bezug auf die Bestimmungen über unerbetene Nachrichten, unter Berücksichtigung des internationalen Umfelds. Hierzu kann die Kommission von den Mitgliedstaaten Informationen einholen, die ohne unangemessene Verzögerung zu liefern sind. Gegebenenfalls unterbreitet die

Kommission unter Berücksichtigung der Ergebnisse des genannten Berichts, etwaiger Änderungen in dem betreffenden Sektor sowie etwaiger weiterer Vorschläge, die sie zur Verbesserung der Wirksamkeit dieser Richtlinie für erforderlich hält, Vorschläge zur Änderung dieser Richtlinie.

Artikel 19
Aufhebung

Die Richtlinie 97/66/EG wird mit Wirkung ab dem in Artikel 17 Absatz 1 genannten Zeitpunkt aufgehoben. Verweisungen auf die aufgehobene Richtlinie gelten als Verweisungen auf die vorliegende Richtlinie.

Artikel 20
Inkrafttreten

Diese Richtlinie tritt am Tag ihrer Veröffentlichung im Amtsblatt der Europäischen Gemeinschaften in Kraft.

Artikel 21
Adressaten

Diese Richtlinie ist an alle Mitgliedstaaten gerichtet.

Anhang 6

Gesetz über Urheberrecht und verwandte Schutzrechte Urheberrechtsgesetz – auszugsweise –

Zum 11. Januar 2018 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: Zuletzt geändert durch Art. 1 G v. 20.12.2016 | 3037

Hinweis: Änderung durch Art. 13 G v. 17.7.2017 | 2541 (Nr. 49) mWv 25.5.2018 durch juris textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

Änderung durch Art. 1 G v. 1.9.2017 | 3346 mWv 1.3.2018 (Nr. 61) durch juris textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

§ 97 Anspruch auf Unterlassung und Schadensersatz

(1) Wer das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht widerrechtlich verletzt, kann von dem Verletzten auf Beseitigung der Beeinträchtigung, bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der Anspruch auf Unterlassung besteht auch dann, wenn eine Zuwiderhandlung erstmalig droht.

(2) Wer die Handlung vorsätzlich oder fahrlässig vornimmt, ist dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet. Bei der Bemessung des Schadensersatzes kann auch der Gewinn, den der Verletzer durch die Verletzung des Rechts erzielt hat, berücksichtigt werden. Der Schadensersatzanspruch kann auch auf der Grundlage des Betrages berechnet werden, den der Verletzer als angemessene Vergütung hätte entrichten müssen, wenn er die Erlaubnis zur Nutzung des verletzten Rechts eingeholt hätte. Urheber, Verfasser wissenschaftlicher Ausgaben (§ 70), Lichtbildner (§ 72) und ausübende Künstler (§ 73) können auch wegen des Schadens, der nicht Vermögensschaden ist, eine Entschädigung in Geld verlangen, wenn und soweit dies der Billigkeit entspricht.

§ 97a Abmahnung

(1) Der Verletzte soll den Verletzer vor Einleitung eines gerichtlichen Verfahrens auf Unterlassung abmahnen und ihm Gelegenheit geben, den Streit durch Abgabe einer mit einer angemessenen Vertragsstrafe bewehrten Unterlassungsverpflichtung beizulegen.

(2) Die Abmahnung hat in klarer und verständlicher Weise

1. Name oder Firma des Verletzten anzugeben, wenn der Verletzte nicht selbst, sondern ein Vertreter abmahnt,

2. die Rechtsverletzung genau zu bezeichnen,

3. geltend gemachte Zahlungsansprüche als Schadensersatz- und Aufwendungsersatzansprüche aufzuschlüsseln und

4. wenn darin eine Aufforderung zur Abgabe einer Unterlassungsverpflichtung enthalten ist, anzugeben, inwieweit die vorgeschlagene Unterlassungsverpflichtung über die abgemahnte Rechtsverletzung hinausgeht.

Eine Abmahnung, die nicht Satz 1 entspricht, ist unwirksam.

(3) Soweit die Abmahnung berechtigt ist und Absatz 2 Satz 1 Nummer 1 bis 4 entspricht, kann der Ersatz der erforderlichen Aufwendungen verlangt werden. Für die Inanspruchnahme anwaltlicher Dienstleistungen beschränkt sich der Ersatz der erforderlichen Aufwendungen hinsichtlich der gesetzlichen Gebühren auf Gebühren nach einem Gegenstandswert für den Unterlassungs- und Beseitigungsanspruch von 1 000 Euro, wenn der Abgemahnte

1. eine natürliche Person ist, die nach diesem Gesetz geschützte Werke oder andere nach diesem Gesetz geschützte Schutzgegenstände nicht für ihre gewerbliche oder selbständige berufliche Tätigkeit verwendet, und

2. nicht bereits wegen eines Anspruchs des Abmahnenden durch Vertrag, auf Grund einer rechtskräftigen gerichtlichen Entscheidung oder einer einstweiligen Verfügung zur Unterlassung verpflichtet ist.

Der in Satz 2 genannte Wert ist auch maßgeblich, wenn ein Unterlassungs- und ein Beseitigungsanspruch nebeneinander geltend gemacht werden. Satz 2 gilt nicht, wenn der genannte Wert nach den besonderen Umständen des Einzelfalles unbillig ist.

(4) Soweit die Abmahnung unberechtigt oder unwirksam ist, kann der Abgemahnte Ersatz der für die Rechtsverteidigung erforderlichen Aufwendungen verlangen, es sei denn, es war für den Abmahnenden zum Zeitpunkt der Abmahnung nicht erkennbar, dass die Abmahnung unberechtigt war. Weiter gehende Ersatzansprüche bleiben unberührt.

§ 101 Anspruch auf Auskunft

(1) Wer in gewerblichem Ausmaß das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht widerrechtlich verletzt, kann von dem Verletzten auf unverzügliche Auskunft über die Herkunft und den Vertriebsweg der rechtsverletzenden Vervielfältigungsstücke oder sonstigen Erzeugnisse in Anspruch genommen werden. Das gewerbliche Ausmaß kann sich sowohl aus der Anzahl der Rechtsverletzungen als auch aus der Schwere der Rechtsverletzung ergeben.

(2) In Fällen offensichtlicher Rechtsverletzung oder in Fällen, in denen der Verletzte gegen den Verletzer Klage erhoben hat, besteht der Anspruch unbeschadet von Absatz 1 auch gegen eine Person, die in gewerblichem Ausmaß

1. rechtsverletzende Vervielfältigungsstücke in ihrem Besitz hatte,

2. rechtsverletzende Dienstleistungen in Anspruch nahm,

3. für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbrachte oder

4. nach den Angaben einer in Nummer 1, 2 oder Nummer 3 genannten Person an der Herstellung, Erzeugung oder am Vertrieb solcher Vervielfältigungsstücke, sonstigen Erzeugnisse oder Dienstleistungen beteiligt war,

es sei denn, die Person wäre nach den §§ 383 bis 385 der Zivilprozessordnung im Prozess gegen den Verletzer zur Zeugnisverweigerung berechtigt. Im Fall der gerichtlichen Geltendmachung des Anspruchs nach Satz 1 kann das Gericht den gegen den Verletzer anhängigen Rechtsstreit auf Antrag bis zur Erledigung des wegen des Auskunftsanspruchs geführten Rechtsstreits aussetzen. Der zur Auskunft Verpflichtete kann von dem Verletzten den Ersatz der für die Auskunftserteilung erforderlichen Aufwendungen verlangen.

(3) Der zur Auskunft Verpflichtete hat Angaben zu machen über

1. Namen und Anschrift der Hersteller, Lieferanten und anderer Vorbesitzer der Vervielfältigungsstücke oder sonstigen Erzeugnisse, der Nutzer der Dienstleistungen sowie der gewerblichen Abnehmer und Verkaufsstellen, für die sie bestimmt waren, und

2. die Menge der hergestellten, ausgelieferten, erhaltenen oder bestellten Vervielfältigungsstücke oder sonstigen Erzeugnisse sowie über die Preise, die für die betreffenden Vervielfältigungsstücke oder sonstigen Erzeugnisse bezahlt wurden.

(4) Die Ansprüche nach den Absätzen 1 und 2 sind ausgeschlossen, wenn die Inanspruchnahme im Einzelfall unverhältnismäßig ist.

(5) Erteilt der zur Auskunft Verpflichtete die Auskunft vorsätzlich oder grob fahrlässig falsch oder unvollständig, so ist er dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet.

(6) Wer eine wahre Auskunft erteilt hat, ohne dazu nach Absatz 1 oder Absatz 2 verpflichtet gewesen zu sein, haftet Dritten gegenüber nur, wenn er wusste, dass er zur Auskunftserteilung nicht verpflichtet war.

(7) In Fällen offensichtlicher Rechtsverletzung kann die Verpflichtung zur Erteilung der Auskunft im Wege der einstweiligen Verfügung nach den §§ 935 bis 945 der Zivilprozessordnung angeordnet werden.

(8) Die Erkenntnisse dürfen in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten wegen einer vor der Erteilung der Auskunft begangenen Tat gegen den Verpflichteten oder gegen einen in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Verpflichteten verwertet werden.

(9) Kann die Auskunft nur unter Verwendung von Verkehrsdaten (§ 3 Nr. 30 des Telekommunikationsgesetzes) erteilt werden, ist für ihre Erteilung eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten erforderlich, die von dem Verletzten zu beantragen ist. Für den Erlass dieser Anordnung ist das Landgericht, in dessen Bezirk der zur Auskunft Verpflichtete seinen Wohnsitz, seinen Sitz oder eine Niederlassung hat, ohne Rücksicht auf den Streitwert ausschließlich zuständig. Die Entscheidung trifft die Zivilkammer. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die Kosten der richterlichen Anordnung trägt der Verletzte. Gegen die Entscheidung des Landgerichts ist die Beschwerde statthaft. Die Beschwerde ist binnen einer Frist von zwei Wochen einzulegen. Die Vorschriften zum Schutz personenbezogener Daten bleiben im Übrigen unberührt.

(10) Durch Absatz 2 in Verbindung mit Absatz 9 wird das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) eingeschränkt.

Anhang 7

Strafprozessordnung – auszugsweise –

Zum 11. Januar 2018 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: Neugefasst durch Bek. v. 7.4.1987 | 1074, 1319
Zuletzt geändert durch Art. 11 Abs. 17 G v. 18.7.2017 | 2745

Hinweis: Änderung durch Art. 3 G v. 17.8.2017 | 3202, 3630 (Nrn. 58 u. 71) durch juris textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

Änderung durch Art. 1 G v. 27.8.2017 | 3295 ist berücksichtigt

Änderung durch Art. 2 G v. 30.10.2017 | 3618 ist berücksichtigt

§ 100a Telekommunikationsüberwachung

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

1. aus dem Strafgesetzbuch:

a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80a bis 82, 84 bis 86, 87 bis 89a, 89c Absatz 1 bis 4, 94 bis 100a,

b) Bestechlichkeit und Bestechung von Mandatsträgern nach § 108e,

c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,

d) Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130,

e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,

f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Absatz 1 und 2, § 184c Absatz 2,

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

i) Straftaten gegen die persönliche Freiheit nach den §§ 232, 232a Absatz 1 bis 5, den §§ 232b, 233 Absatz 2, den §§ 233a, 234, 234a, 239a und 239b,

j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,

k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,

l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,

m) Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4; beruht die Strafbarkeit darauf, dass die Straflosigkeit nach § 261 Absatz 9 Satz 2 gemäß § 261 Absatz 9 Satz 3 ausgeschlossen ist, jedoch nur dann, wenn der Gegenstand aus einer der in den Nummern 1 bis 11 genannten schweren Straftaten herrührt,

n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,

o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,

p) Sportwettbetrug und Manipulation von berufssportlichen Wettbewerben unter den in § 265e Satz 2 genannten Voraussetzungen,

q) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,

r) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,

s) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,

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

u) Bestechlichkeit und Bestechung nach den §§ 332 und 334,

2. aus der Abgabenordnung:

a) Steuerhinterziehung unter den in § 370 Abs. 3 Satz 2 Nr. 5 genannten Voraussetzungen,

b) gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,

c) Steuerhehlerei im Falle des § 374 Abs. 2,

3. aus dem Anti-Doping-Gesetz:

Straftaten nach § 4 Absatz 4 Nummer 2 Buchstabe b,

4. aus dem Asylgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,

5. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Abs. 2,

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

6. aus dem Außenwirtschaftsgesetz:

vorsätzliche Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes,

7. aus dem Betäubungsmittelgesetz:

a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,

b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,

8. aus dem Grundstoffüberwachungsgesetz:

Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,

9. aus dem Gesetz über die Kontrolle von Kriegswaffen:

   a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,

   b) Straftaten nach § 22a Abs. 1 bis 3,

9a. aus dem Neue-psychoaktive-Stoffe-Gesetz:

Straftaten nach § 4 Absatz 3 Nummer 1 Buchstabe a,

10. aus dem Völkerstrafgesetzbuch:

   a) Völkermord nach § 6,

   b) Verbrechen gegen die Menschlichkeit nach § 7,

   c) Kriegsverbrechen nach den §§ 8 bis 12,

   d) Verbrechen der Aggression nach § 13,

11. aus dem Waffengesetz:

   a) Straftaten nach § 51 Abs. 1 bis 3,

   b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.

(4) Auf Grund der Anordnung einer Überwachung und Aufzeichnung der Telekommunikation hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) diese Maßnahmen zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Absatz 2 gilt entsprechend.

(5) Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:

   a) die laufende Telekommunikation (Absatz 1 Satz 2), oder

b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),

2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(6) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

§ 100b Online-Durchsuchung

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,

2. die Tat auch im Einzelfall besonders schwer wiegt und

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Besonders schwere Straftaten im Sinne des Absatzes 1 Nummer 1 sind:

1. aus dem Strafgesetzbuch:

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

b) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,

c) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,

d) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176a Absatz 2 Nummer 2 oder Absatz 3 und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

e) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184b Absatz 2,

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

g) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, der §§ 239a, 239b und Menschenhandel nach § 232 Absatz 3, Zwangsprostitution und Zwangsarbeit nach § 232a Absatz 3, 4 oder 5 zweiter Halbsatz, § 232b Absatz 3 oder 4 in Verbindung mit § 232a Absatz 4 oder 5 zweiter Halbsatz und Ausbeutung unter Ausnutzung einer Freiheitsberaubung nach § 233a Absatz 3 oder 4 zweiter Halbsatz,

h) Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a,

i) schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251,

j) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen,

k) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,

l) besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Absatz 4 Satz 2 genannten Voraussetzungen; beruht die Strafbarkeit darauf, dass die Straflosigkeit nach § 261 Absatz 9 Satz 2 gemäß § 261 Absatz 9 Satz 3 ausgeschlossen ist, jedoch nur dann, wenn der Gegenstand aus einer der in den Nummern 1 bis 7 genannten besonders schweren Straftaten herrührt,

m) besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Absatz 1 unter den in § 335 Absatz 2 Nummer 1 bis 3 genannten Voraussetzungen,

2. aus dem Asylgesetz:

   a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Absatz 3,

   b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a Absatz 1,

3. aus dem Aufenthaltsgesetz:

   a) Einschleusen von Ausländern nach § 96 Absatz 2,

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

4. aus dem Betäubungsmittelgesetz:

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

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

5. aus dem Gesetz über die Kontrolle von Kriegswaffen:

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

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

6. aus dem Völkerstrafgesetzbuch:

   a) Völkermord nach § 6,

   b) Verbrechen gegen die Menschlichkeit nach § 7,

   c) Kriegsverbrechen nach den §§ 8 bis 12,

   d) Verbrechen der Aggression nach § 13,

7. aus dem Waffengesetz:

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

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

(3) Die Maßnahme darf sich nur gegen den Beschuldigten richten. Ein Eingriff in informationstechnische Systeme anderer Personen ist nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte informationstechnische Systeme der anderen Person benutzt, und

2. die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(4) § 100a Absatz 5 und 6 gilt mit Ausnahme von Absatz 5 Satz 1 Nummer 1 entsprechend.

§ 100c Akustische Wohnraumüberwachung

(1) Auch ohne Wissen der Betroffenen darf das in einer Wohnung nichtöffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,

2. die Tat auch im Einzelfall besonders schwer wiegt,

3. auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind, und

4. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre.

(2) Die Maßnahme darf sich nur gegen den Beschuldigten richten und nur in Wohnungen des Beschuldigten durchgeführt werden. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte sich dort aufhält und

2. die Maßnahme in Wohnungen des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

§ 100e Verfahren bei Maßnahmen nach den §§ 100a bis 100c

(1) Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) Maßnahmen nach den §§ 100b und 100c dürfen nur auf Antrag der Staatsanwaltschaft durch die in § 74a Absatz 4 des Gerichtsverfassungsgesetzes genannte Kammer des Landgerichts angeordnet werden, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat. Bei Gefahr im Verzug kann diese Anordnung auch durch den Vorsitzenden getroffen werden. Dessen Anordnung tritt außer Kraft, wenn sie nicht binnen drei Werktagen von der Strafkammer bestätigt wird. Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Ist die Dauer der Anordnung auf insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen das Oberlandesgericht.

(3) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,

2. der Tatvorwurf, auf Grund dessen die Maßnahme angeordnet wird,

3. Art, Umfang, Dauer und Endzeitpunkt der Maßnahme,

4. die Art der durch die Maßnahme zu erhebenden Informationen und ihre Bedeutung für das Verfahren,

5. bei Maßnahmen nach § 100a die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist; im Fall des § 100a Absatz 1 Satz 2 und 3 eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das eingegriffen werden soll,

6. bei Maßnahmen nach § 100b eine möglichst genaue Bezeichnung des informationstechnischen Systems, aus dem Daten erhoben werden sollen,

7. bei Maßnahmen nach § 100c die zu überwachende Wohnung oder die zu überwachenden Wohnräume.

(4) In der Begründung der Anordnung oder Verlängerung von Maßnahmen nach den §§ 100a bis 100c sind deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen anzugeben:

1. die bestimmten Tatsachen, die den Verdacht begründen,

2. die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme,

3. bei Maßnahmen nach § 100c die tatsächlichen Anhaltspunkte im Sinne des § 100d Absatz 4 Satz 1.

(5) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Das anordnende Gericht ist nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten. Bei Maßnahmen nach den §§ 100b und 100c ist das anordnende Gericht auch über den Verlauf zu unterrichten. Liegen die Voraussetzungen der Anordnung nicht mehr vor, so hat das Gericht den Abbruch der Maßnahme anzuordnen, sofern der Abbruch nicht bereits durch die Staatsanwaltschaft veranlasst wurde. Die Anordnung des Abbruchs einer Maßnahme nach den §§ 100b und 100c kann auch durch den Vorsitzenden erfolgen.

(6) Die durch Maßnahmen nach den §§ 100b und 100c erlangten und verwertbaren personenbezogenen Daten dürfen für andere Zwecke nach folgenden Maßgaben verwendet werden:

1. Die Daten dürfen in anderen Strafverfahren ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer Maßnahmen nach § 100b oder § 100c angeordnet werden könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.

2. Die Verwendung der Daten, auch solcher nach § 100d Absatz 5 Satz 1 zweiter Halbsatz, zu Zwecken der Gefahrenabwehr ist nur zur Abwehr einer im Einzelfall bestehenden Lebensgefahr oder einer dringenden Gefahr für Leib oder Freiheit einer Person, für die Sicherheit oder den Bestand des Staates oder für Gegenstände von bedeutendem Wert, die der Versorgung der Bevölkerung dienen, von kulturell herausragendem Wert oder in § 305 des Strafgesetzbuches genannt sind, zulässig. Die Daten dürfen auch zur Abwehr einer im Einzelfall bestehenden dringenden Gefahr für sonstige bedeutende Vermögenswerte verwendet werden. Sind die Daten zur Abwehr der Gefahr oder für eine vorgerichtliche oder gerichtliche Überprüfung der zur Gefahrenabwehr getroffenen Maßnahmen nicht mehr erforderlich, so sind Aufzeichnungen über diese Daten von der für die Gefahrenabwehr zuständigen Stelle unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige vorgerichtliche oder gerichtliche Überprüfung zurückgestellt ist, dürfen die Daten nur für diesen Zweck verwendet werden; für eine Verwendung zu anderen Zwecken sind sie zu sperren.

3. Sind verwertbare personenbezogene Daten durch eine entsprechende polizeirechtliche Maßnahme erlangt worden, dürfen sie in einem Strafverfahren ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer die Maßnahmen nach § 100b oder § 100c angeordnet werden könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.

§ 100g Erhebung von Verkehrsdaten

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

2. eine Straftat mittels Telekommunikation begangen hat,

so dürfen Verkehrsdaten (§ 96 Absatz 1 des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Im Fall des Satzes 1 Nummer 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Die Erhebung von Standortdaten ist nach diesem Absatz nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nummer 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, und wiegt die Tat auch im Einzelfall besonders schwer, dürfen die nach § 113b des Telekommunikationsgesetzes gespeicherten Verkehrsdaten erhoben werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Besonders schwere Straftaten im Sinne des Satzes 1 sind:

1. aus dem Strafgesetzbuch:

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

   b) besonders schwerer Fall des Landfriedensbruchs nach § 125a, Bildung krimineller Ver-

einigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 Alternative 1, jeweils auch in Verbindung mit § 129b Absatz 1,

c) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

d) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften in den Fällen des § 184b Absatz 2, § 184c Absatz 2,

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

f) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, §§ 239a, 239b und Zwangsprostitution und Zwangsarbeit nach § 232a Absatz 3, 4 oder 5 zweiter Halbsatz, § 232b Absatz 3 oder 4 in Verbindung mit § 232a Absatz 4 oder 5 zweiter Halbsatz und Ausbeutung unter Ausnutzung einer Freiheitsberaubung nach § 233a Absatz 3 oder 4 zweiter Halbsatz,

g) Einbruchdiebstahl in eine dauerhaft genutzte Privatwohnung nach § 244 Absatz 4, schwerer Bandendiebstahl nach § 244a Absatz 1, schwerer Raub nach § 250 Absatz 1 oder Absatz 2, Raub mit Todesfolge nach § 251, räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen, gewerbsmäßige Bandenhehlerei nach § 260a Absatz 1, besonders schwerer Fall der Geldwäsche und der Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Absatz 4 Satz 2 genannten Voraussetzungen,

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

2. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Absatz 2,

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

3. aus dem Außenwirtschaftsgesetz:

Straftaten nach § 17 Absatz 1 bis 3 und § 18 Absatz 7 und 8,

4. aus dem Betäubungsmittelgesetz:

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

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

5. aus dem Grundstoffüberwachungsgesetz:

   eine Straftat nach § 19 Absatz 1 unter den in § 19 Absatz 3 Satz 2 genannten Voraussetzungen,

6. aus dem Gesetz über die Kontrolle von Kriegswaffen:

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

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

7. aus dem Völkerstrafgesetzbuch:

   a) Völkermord nach § 6,

   b) Verbrechen gegen die Menschlichkeit nach § 7,

   c) Kriegsverbrechen nach den §§ 8 bis 12,

   d) Verbrechen der Aggression nach § 13,

8. aus dem Waffengesetz:

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

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

(3) Die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten (Funkzellenabfrage) ist nur zulässig,

1. wenn die Voraussetzungen des Absatzes 1 Satz 1 Nummer 1 erfüllt sind,

2. soweit die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht und

3. soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

   Auf nach § 113b des Telekommunikationsgesetzes gespeicherte Verkehrsdaten darf für eine Funkzellenabfrage nur unter den Voraussetzungen des Absatzes 2 zurückgegriffen werden.

(4) Die Erhebung von Verkehrsdaten nach Absatz 2, auch in Verbindung mit Absatz 3 Satz 2, die sich gegen eine der in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannten Personen richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, ist unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist aktenkundig zu machen. Die Sätze 2 bis 4 gelten ent-

sprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannte Person richtet, von dieser Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. § 160a Absatz 3 und 4 gilt entsprechend.

(5) Erfolgt die Erhebung von Verkehrsdaten nicht beim Erbringer öffentlich zugänglicher Telekommunikationsdienste, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

§ 100i Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, so dürfen durch technische Mittel

1. die Gerätenummer eines Mobilfunkendgerätes und die Kartennummer der darin verwendeten Karte sowie
2. der Standort eines Mobilfunkendgerätes

ermittelt werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(3) § 100a Abs. 3 und § 100e Absatz 1 Satz 1 bis 3, Absatz 3 Satz 1 und Absatz 5 Satz 1 gelten entsprechend. Die Anordnung ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen fortbestehen.

§ 100j Bestandsdatenauskunft

(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in

diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3, § 113c Absatz 1 Nummer 3 des Telekommunikationsgesetzes).

(3) Auskunftsverlangen nach Absatz 1 Satz 2 dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Die Sätze 1 bis 3 finden keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.

(4) Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 über die Beauskunftung zu benachrichtigen. Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(5) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. § 95 Absatz 2 gilt entsprechend.

Anhang 8

Strafgesetzbuch – auszugsweise –

Zum 11. Januar 2018 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: Neugefasst durch Bek. v. 13.11.1998 | 3322;
zuletzt geändert durch Art. 1 G v. 30.10.2017 | 3618

Hinweis: Berichtigung vom 1.11.2017 | 3630 ist berücksichtigt

§ 201 Verletzung der Vertraulichkeit des Wortes

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder

2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder

2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

   Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

(3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter die Vertraulichkeit des Wortes verletzt (Absätze 1 und 2).

(4) Der Versuch ist strafbar.

(5) Die Tonträger und Abhörgeräte, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,

2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

Anhang 9

Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation

(Telekommunikations-Überwachungsverordnung)

Zum 11. Januar 2018 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: Neugefasst durch Bek. v. 11.7.2017 | 2316

Hinweis: Änderung durch Art. 16 G v. 17.8.2017 | 3202 mWv 24.8.2017 (Nr. 58) durch juris noch nicht berücksichtigt

Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

Fußnote

(+++ Textnachweis ab: 9.11.2005 +++)

(+++ Amtlicher Hinweis des Normgebers auf EG-Recht:

Notifizierung gem. der EURL 2015/1535 (CELEX Nr: 32015L1535) +++)

Teil 1 Allgemeine Vorschriften

Neugefasst durch Bek. v. 11.7.2017 | 2316

§ 1 Gegenstand der Verordnung

Diese Verordnung regelt

1. die grundlegenden Anforderungen an die Gestaltung der technischen Einrichtungen, die für die Umsetzung der

   a) in den §§ 100a und 100b der Strafprozessordnung,

   b) in den §§ 3, 5 und 8 des Artikel 10-Gesetzes,

   c) in den §§ 23a bis 23c und 23e des Zollfahndungsdienstgesetzes,

   d) in § 20l** des Bundeskriminalamtgesetzes,

e) in den §§ 6, 12 und 14 des BND-Gesetzes sowie

f) im Landesrecht

vorgesehenen Maßnahmen zur Überwachung der Telekommunikation erforderlich sind, sowie organisatorische Eckpunkte für die Umsetzung derartiger Maßnahmen mittels dieser Einrichtungen,

2. den Rahmen für die Technische Richtlinie nach § 110 Absatz 3 des Telekommunikationsgesetzes,

3. das Verfahren für den Nachweis nach § 110 Absatz 1 Satz 1 Nummer 3 und 4 des Telekommunikationsgesetzes,

4. die Ausgestaltung der Verpflichtungen zur Duldung der Aufstellung von technischen Einrichtungen für Maßnahmen der strategischen Kontrolle nach § 5 oder § 8 des Artikel 10-Gesetzes oder nach den §§ 6, 12 oder 14 des BND-Gesetzes sowie des Zugangs zu diesen Einrichtungen,

5. bei welchen Telekommunikationsanlagen dauerhaft oder vorübergehend keine technischen Einrichtungen zur Umsetzung von Anordnungen zur Überwachung der Telekommunikation vorgehalten oder keine organisatorischen Vorkehrungen getroffen werden müssen,

6. welche Ausnahmen von der Erfüllung einzelner technischer Anforderungen die Bundesnetzagentur zulassen kann,

7. die Anforderungen an die Aufzeichnungsanschlüsse, an die die Aufzeichnungs- und Auswertungseinrichtungen angeschlossen werden, sowie

8. die Anforderungen an das Übermittlungsverfahren und das Datenformat für Auskunftsersuchen über Verkehrsdaten und der zugehörigen Ergebnisse.

** Gemäß Artikel 10 in Verbindung mit Artikel 13 Absatz 1 Satz 1 des Gesetzes vom 1. Juni 2017 (BGBl. | S. 1354) wird am 25. Mai 2018 in § 1 Absatz 1 Nummer 1 Buchstabe d die Angabe „§ 201“ durch die Angabe „§ 51“ ersetzt.

§ 2 Begriffsbestimmungen

Im Sinne dieser Verordnung ist

1. Anordnung

a) im Sinne der Teile 2 und 3 die Anordnung zur Überwachung der Telekommunikation nach § 100b der Strafprozessordnung, § 10 des Artikel 10-Gesetzes, § 23b des Zollfahndungs-

dienstgesetzes, § 20l des Bundeskriminalamtgesetzes, § 9 des BND-Gesetzes oder nach Landesrecht und

b) im Sinne des Teils 4 die Anordnung zur Erteilung von Auskünften über Verkehrsdaten nach § 100g in Verbindung mit § 101a Absatz 1 der Strafprozessordnung, § 8a Absatz 2 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes, auch in Verbindung mit § 4a des MAD-Gesetzes oder § 3 des BND-Gesetzes, § 20m des Bundeskriminalamtgesetzes, § 23g des Zollfahndungsdienstgesetzes oder nach Landesrecht;

2. Aufzeichnungsanschluss

der Telekommunikationsanschluss einer berechtigten Stelle, an den deren Aufzeichnungs- und Auswertungseinrichtungen angeschlossen werden (Netzabschlusspunkt im Sinne von § 110 Absatz 6 des Telekommunikationsgesetzes);

2a. Aufzeichnungs- und Auswertungseinrichtung

die technische Einrichtung einer berechtigten Stelle, die an Aufzeichnungsanschlüsse angeschlossen wird und der Aufzeichnung, technischen Aufbereitung und Auswertung der Überwachungskopie dient;

3. berechtigte Stelle

a) im Sinne der Teile 2 und 3 die nach § 100b Absatz 3 Satz 1 der Strafprozessordnung, § 1 Absatz 1 Nummer 1 des Artikel 10-Gesetzes, § 23a Absatz 1 Satz 1 des Zollfahndungsdienstgesetzes, § 20l Absatz 5 Satz 1 des Bundeskriminalamtgesetzes, den §§ 6, 12 oder 14 des BND-Gesetzes oder nach Landesrecht auf Grund der jeweiligen Anordnung zur Überwachung und Aufzeichnung der Telekommunikation berechtigte Stelle und

b) im Sinne des Teils 4 die Stelle,

aa) die nach § 101a Absatz 1 in Verbindung mit § 100b der Strafprozessordnung, § 8a Absatz 2 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes, auch in Verbindung mit § 4a des MAD-Gesetzes oder § 3 des BND-Gesetzes, § 20m des Bundeskriminalamtgesetzes, § 23g des Zollfahndungsdienstgesetzes oder nach Landesrecht auf Grund der jeweiligen Anordnung berechtigt ist, Auskunftsverlangen über nach § 96 des Telekommunikationsgesetzes erhobene Verkehrsdaten zu stellen, oder

bb) der nach § 113c Absatz 1 Nummer 1 oder 2 des Telekommunikationsgesetzes Auskünfte über nach § 113b des Telekommunikationsgesetzes gespeicherte Verkehrsdaten erteilt werden dürfen;

4. Betreiber einer Telekommunikationsanlage

das Unternehmen, das die tatsächliche Kontrolle über die Funktionen einer Telekommunikationsanlage ausübt;

5. (weggefallen)

6. Endgerät

   die technische Einrichtung, mittels derer ein Nutzer einen Telekommunikationsanschluss zur Abwicklung seiner Telekommunikation nutzt;

7. Pufferung

   die kurzzeitige Zwischenspeicherung von Informationen zur Vermeidung von Informationsverlusten während systembedingter Wartezeiten;

8. Referenznummer

   die von der berechtigten Stelle vorgegebene eindeutige, auch nichtnumerische Bezeichnung der Überwachungsmaßnahme oder des Auskunftsverlangens, die auch die Bezeichnung der berechtigten Stelle enthält;

9. Speichereinrichtung

   eine netzseitige Einrichtung zur Speicherung von Telekommunikation, die einem Teilnehmer oder sonstigen Nutzer zugeordnet ist;

10. Telekommunikationsanschluss

    der durch eine Rufnummer oder andere Adressierungsangabe eindeutig bezeichnete Zugang zu einer Telekommunikationsanlage, der es einem Nutzer ermöglicht, Telekommunikationsdienste zu nutzen;

11. Übergabepunkt

    der Punkt der technischen Einrichtungen des Verpflichteten, an dem er die Überwachungskopie bereitstellt; der Übergabepunkt kann als systeminterner Übergabepunkt gestaltet sein, der am Ort der Telekommunikationsanlage nicht physikalisch dargestellt ist;

12. Übertragungsweg, der dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dient

    die Verbindung zwischen dem Endgerät eines Internet-Nutzers und dem Netzknoten, der den Koppelpunkt zum Internet enthält, soweit nicht die Vermittlungsfunktion eines Netzknotens genutzt wird, der dem Zugang zum Telefonnetz dient;

13. Überwachungseinrichtung

    die für die technische Umsetzung von Anordnungen erforderlichen technischen Einrichtungen des Betreibers einer Telekommunikationsanlage einschließlich der zugehörigen Programme und Daten;

14. Überwachungskopie

das vom Verpflichteten auf Grund einer Anordnung auszuleitende und an die Aufzeichnungs- und Auswertungseinrichtung zu übermittelnde Doppel der zu überwachenden Telekommunikation;

15. Überwachungsmaßnahme

eine Maßnahme zur Überwachung der Telekommunikation nach den §§ 100a, 100b der Strafprozessordnung, den §§ 3, 5 oder 8 des Artikel 10-Gesetzes, den §§ 23a bis 23c des Zollfahndungsdienstgesetzes, § 20l des Bundeskriminalamtgesetzes, den §§ 6, 12 oder 14 des BND-Gesetzes oder nach Landesrecht;

16. Verpflichteter

wer nach dieser Verordnung technische oder organisatorische Vorkehrungen zur Umsetzung von Anordnungen zu treffen hat;

17. zu überwachende Kennung

a) das technische Merkmal, durch das die zu überwachende Telekommunikation in der Telekommunikationsanlage des Verpflichteten gekennzeichnet ist,

b) im Falle von Übertragungswegen, die dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dienen, oder im Falle des § 5 oder des § 8 des Artikel 10-Gesetzes die Bezeichnung des Übertragungswegs, oder

c) im Falle der §§ 6, 12 oder 14 des BND-Gesetzes die Bezeichnung des Telekommunikationsnetzes einschließlich der für die Umsetzung der Anordnung erforderlichen, in der Technischen Richtlinie nach § 110 Absatz 3 des Telekommunikationsgesetzes festgelegten technischen Parameter;

18. Zuordnungsnummer

das vom Verpflichteten zu vergebende eindeutige, auch nichtnumerische Zuordnungsmerkmal, auf Grund dessen Teile der Überwachungskopie und die zugehörigen Daten einander zweifelsfrei zugeordnet werden können.

Teil 2 Maßnahmen nach den §§ 100a, 100b der Strafprozessordnung, § 3 des Artikel 10-Gesetzes, den §§ 23a bis 23c und 23e des Zollfahndungsdienstgesetzes, § 20l des Bundeskriminalamtgesetzes oder nach Landesrecht

Abschnitt 1 Kreis der Verpflichteten, Grundsätze

§ 3 Kreis der Verpflichteten

(1) Die Vorschriften dieses Teils gelten für die Betreiber von Telekommunikationsanlagen, mit denen öffentlich zugängliche Telekommunikationsdienste erbracht werden. Werden mit einer Telekommunikationsanlage sowohl öffentlich zugängliche Telekommunikationsdienste als auch andere Telekommunikationsdienste erbracht, gelten die Vorschriften nur für den Teil der Telekommunikationsanlage, der der Erbringung von öffentlich zugänglichen Telekommunikationsdiensten dient.

(2) Für Telekommunikationsanlagen im Sinne von Absatz 1 müssen keine Vorkehrungen getroffen werden, soweit

1. es sich um ein Telekommunikationsnetz handelt, das Teilnehmernetze miteinander verbindet und keine Telekommunikationsanschlüsse aufweist,

2. sie Netzknoten sind, die der Zusammenschaltung mit dem Internet dienen,

3. sie aus Übertragungswegen gebildet werden, es sei denn, dass diese dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dienen,

4. sie ausschließlich der Verteilung von Rundfunk oder anderen für die Öffentlichkeit bestimmten Diensten, dem Abruf von allgemein zugänglichen Informationen oder der Übermittlung von Messwerten, nicht individualisierten Daten, Notrufen oder Informationen für die Sicherheit und Leichtigkeit des See- oder Luftverkehrs dienen,

5. an sie nicht mehr als 10 000 Teilnehmer oder sonstige Endnutzer angeschlossen sind oder

6. mit ihnen ausschließlich Dienste der elektronischen Post oder ausschließlich nichtkennungsbezogene Internetzugangsdienste über ein drahtloses lokales Netzwerk erbracht werden und an sie nicht mehr als 100 000 Teilnehmer oder sonstige Endnutzer angeschlossen sind.

Satz 1 Nummer 1 und 5 gilt nicht für Netzknoten, die der Vermittlung eines öffentlich zugänglichen Telefondienstes ins Ausland dienen. *3*Satz 1 Nummer 1 und 2 gilt nicht im Hinblick auf Vorkehrungen zur Erfüllung der Verpflichtung aus § 110 Absatz 1 Satz 1 Nummer 1a des Telekommunikationsgesetzes.

(3) § 100b Absatz 3 Satz 1 der Strafprozessordnung, § 2 Absatz 1 Satz 3 des Artikel 10-Gesetzes, § 23a Absatz 8 des Zollfahndungsdienstgesetzes, § 20l Absatz 5 Satz 1 des Bundeskriminal-

amtgesetzes sowie die Vorschriften des Landesrechts über Maßnahmen zur Überwachung der Telekommunikation bleiben von den Absätzen 1 und 2 unberührt.

§ 4 Grenzen des Anwendungsbereichs

(1) Telekommunikation, bei der die Telekommunikationsanlage im Rahmen der üblichen Betriebsverfahren erkennt, dass sich das Endgerät, das die zu überwachende Kennung nutzt, im Ausland befindet, ist nicht zu erfassen, es sei denn, die zu überwachende Telekommunikation

1. wird an einen im Inland gelegenen Telekommunikationsanschluss gerichtet,
2. geht von einem im Inland gelegenen Telekommunikationsanschluss aus oder
3. wird an eine im Inland befindliche Speichereinrichtung um- oder weitergeleitet.

(2) Die Telekommunikation ist jedoch in den Fällen zu erfassen, in denen sie

1. von einem den berechtigten Stellen nicht bekannten Telekommunikationsanschluss im Inland herrührt und für eine in der Anordnung angegebene ausländische Rufnummer bestimmt ist oder
2. von einem in der Anordnung angegebenen Telekommunikationsanschluss im Ausland herrührt und für eine den berechtigten Stellen nicht bekannte Rufnummer im Inland bestimmt ist.

Die technische Umsetzung derartiger Anordnungen ist vom Verpflichteten in Abstimmung mit der Bundesnetzagentur zu regeln, wobei hinsichtlich der Gestaltung der Überwachungseinrichtung, des Übergabepunktes und der zu treffenden organisatorischen Vorkehrungen von § 5 Absatz 1 Nummer 1, § 6 Absatz 3 und 4, § 7 Absatz 1 Satz 1 Nummer 2, 4 und 7 und Absatz 2 bis 4 abgewichen werden kann. § 22 ist im Rahmen von Überwachungsmaßnahmen nach Satz 1 nicht anzuwenden.

§ 5 Grundsätze

(1) Die zu überwachende Telekommunikation umfasst bei Überwachungsmaßnahmen nach den §§ 100a, 100b der Strafprozessordnung, dem § 3 des Artikel 10-Gesetzes, den §§ 23a bis 23c des Zollfahndungsdienstgesetzes, § 20l des Bundeskriminalamtgesetzes oder nach Landesrecht die Telekommunikation, die

1. von der zu überwachenden Kennung ausgeht,
2. für die zu überwachende Kennung bestimmt ist,

3. in eine Speichereinrichtung, die der zu überwachenden Kennung zugeordnet ist, eingestellt oder aus dieser abgerufen wird oder

4. (weggefallen)

5. zu einer der zu überwachenden Kennung aktuell zugeordneten anderen Zieladresse um- oder weitergeleitet wird,

und besteht aus dem Inhalt und den Daten über die näheren Umstände der Telekommunikation.

(2) Zur technischen Umsetzung einer Anordnung hat der Verpflichtete der berechtigten Stelle am Übergabepunkt eine vollständige Kopie der durch die zu überwachende Kennung bezeichneten Telekommunikation bereitzustellen, die über seine Telekommunikationsanlage abgewickelt wird. Dabei hat er sicherzustellen, dass die bereitgestellten Daten ausschließlich die durch die Anordnung bezeichnete Telekommunikation enthalten. Bei Zusammenschaltungen mit Telekommunikationsnetzen anderer Betreiber hat er sicherzustellen, dass die Daten nach § 7 Absatz 1 Satz 1 Nummer 3 im Rahmen der technischen Möglichkeiten übergeben werden. Satz 1 gilt nicht für Telekommunikation, die in rundfunkähnlicher Weise für alle Nutzer gleichermaßen und unverändert übermittelt und vom Verpflichteten selbst eingespeist wird.

(3) Der Verpflichtete hat sicherzustellen, dass er die Umsetzung einer Anordnung eigenverantwortlich vornehmen kann. In diesem Rahmen ist die Wahrnehmung der im Überwachungsfall erforderlichen Tätigkeiten durch einen Erfüllungsgehilfen zulässig, der jedoch nicht der berechtigten Stelle angehören darf.

(4) Der Verpflichtete hat sicherzustellen, dass die technische Umsetzung einer Anordnung weder von den an der Telekommunikation Beteiligten noch von Dritten feststellbar ist. Insbesondere dürfen die Betriebsmöglichkeiten des Telekommunikationsanschlusses, der durch die zu überwachende Kennung genutzt wird, durch die technische Umsetzung einer Anordnung nicht verändert werden.

(5) Der Verpflichtete hat der berechtigten Stelle unmittelbar nach Abschluss der für die technische Umsetzung einer Anordnung erforderlichen Tätigkeiten den tatsächlichen Einrichtungszeitpunkt sowie die tatsächlich betroffene Kennung mitzuteilen. Dies gilt entsprechend für die Übermittlung einer Information zum Zeitpunkt der Beendigung einer Überwachungsmaßnahme.

(6) Der Verpflichtete hat Engpässe, die bei gleichzeitiger Durchführung mehrerer Überwachungsmaßnahmen auftreten, unverzüglich zu beseitigen.

Abschnitt 2 Technische Anforderungen

§ 6 Grundlegende Anforderungen an die technischen Einrichtungen

(1) Der Verpflichtete hat seine Überwachungseinrichtungen so zu gestalten, dass er eine Anordnung unverzüglich umsetzen kann; dies gilt für eine von der berechtigten Stelle verlangte vorfristige Abschaltung einer Überwachungsmaßnahme entsprechend.

(2) Der Verpflichtete hat sicherzustellen, dass die Verfügbarkeit seiner Überwachungseinrichtungen der Verfügbarkeit seiner Telekommunikationsanlage entspricht, soweit dies mit vertretbarem Aufwand realisierbar ist.

(3) Der Verpflichtete hat seine Überwachungseinrichtungen so zu gestalten, dass er die Überwachung neben der in seiner Telekommunikationsanlage verwendeten Ursprungs- oder Zieladresse auf Grund jeder in der Technischen Richtlinie nach § 36 bereichsspezifisch festgelegten Kennungsart ermöglichen kann, die er für die technische Abwicklung der Telekommunikation in seiner Telekommunikationsanlage erhebt. Soweit die zu überwachende Kennung des Telekommunikationsanschlusses in Fällen abgehender Telekommunikation durch die Telekommunikationsanlage des Verpflichteten nicht ausgewertet wird, hat der Verpflichtete die Überwachungskopie nach Maßgabe der Technischen Richtlinie auf der Basis der zugehörigen Benutzerkennung bereitzustellen.

(4) Der Verpflichtete muss sicherstellen, dass er die Überwachung derselben zu überwachenden Kennung gleichzeitig für mehr als eine berechtigte Stelle ermöglichen kann.

§ 7 Bereitzustellende Daten

(1) Der Verpflichtete hat der berechtigten Stelle als Teil der Überwachungskopie auch die folgenden bei ihm vorhandenen Daten bereitzustellen, auch wenn die Übermittlung von Telekommunikationsinhalten nicht zustande kommt:

1. die zu überwachende Kennung;

2. in Fällen, in denen die Telekommunikation von der zu überwachenden Kennung ausgeht,

a) die jeweils gewählte Rufnummer oder andere Adressierungsangabe, auch wenn diese bei vorzeitiger Beendigung eines im Telekommunikationsnetz begonnenen Telekommunikationsversuches unvollständig bleibt und

b) sofern die zu überwachende Telekommunikation an ein anderes als das von dem Nutzer der zu überwachenden Kennung gewählte Ziel um- oder weitergeleitet wird, auch die Rufnummer oder andere Adressierungsangabe des Um- oder Weiterleitungsziels, bei mehrfach gestaffelten Um- oder Weiterleitungen die Rufnummern oder anderen Adressierungsangaben der einzelnen Um- oder Weiterleitungsziele;

3. in Fällen, in denen die zu überwachende Kennung Ziel der Telekommunikation ist, die Rufnummer oder andere Adressierungsangabe, von der die zu überwachende Telekommunikation ausgeht, auch wenn die Telekommunikation an eine andere, der zu überwachenden Kennung aktuell zugeordnete Zieladresse um- oder weitergeleitet wird oder das Ziel eine der zu überwachenden Kennung zugeordnete Speichereinrichtung ist;

4. in Fällen, in denen die zu überwachende Kennung zeitweise einem beliebigen Telekommunikationsanschluss zugeordnet ist, auch die diesem Anschluss fest zugeordnete Rufnummer oder andere Adressierungsangabe;

5. in Fällen, in denen der Nutzer für eine bestimmte Telekommunikation ein Dienstmerkmal in Anspruch nimmt, die Angabe dieses Dienstmerkmals einschließlich dessen Kenngrößen, soweit diese Angaben in dem Netzknoten vorhanden sind, in dem die Anordnung umgesetzt wird;

6. Angaben über die technische Ursache für die Beendigung der zu überwachenden Telekommunikation oder für das Nichtzustandekommen einer von der zu überwachenden Kennung veranlassten Telekommunikation, soweit diese Angaben in dem Netzknoten vorhanden sind, in dem die Anordnung umgesetzt wird;

7. bei einer zu überwachenden Kennung, deren Nutzung nicht ortsgebunden ist, Angaben zum Standort des Endgerätes mit der größtmöglichen Genauigkeit, die in dem das Endgerät versorgenden Netz für diesen Standort üblicherweise zur Verfügung steht; zur Umsetzung von Anordnungen, durch die Angaben zum Standort des empfangsbereiten, der zu überwachenden Kennung zugeordneten Endgerätes verlangt werden, hat der Verpflichtete seine Überwachungseinrichtungen so zu gestalten, dass sie diese Angaben automatisch erfassen und an die berechtigte Stelle weiterleiten;

8. Angaben zur Zeit (auf der Grundlage der amtlichen Zeit), zu der die zu überwachende Telekommunikation stattgefunden hat,

   a) in Fällen, in denen die zu überwachende Telekommunikation über physikalische oder logische Kanäle übermittelt wird (verbindungsorientierte Telekommunikation), mindestens zwei der folgenden Angaben:

      aa) Datum und Uhrzeit des Beginns der Telekommunikation oder des Telekommunikationsversuchs,

      bb) Datum und Uhrzeit des Endes der Telekommunikation,

      cc) Dauer der Telekommunikation,

   b) in Fällen, in denen die zu überwachende Telekommunikation nicht über physikalische oder logische Kanäle übermittelt wird (verbindungslose Telekommunikation), die

Zeitpunkte mit Datum und Uhrzeit, zu denen die einzelnen Bestandteile der zu überwachenden Telekommunikation an die zu überwachende Kennung oder von der zu überwachenden Kennung gesendet werden;

9. die der Telekommunikationsanlage des Verpflichteten bekannten öffentlichen Internetprotokoll-Adressen der beteiligten Nutzer;

10. die der Telekommunikationsanlage des Verpflichteten bekannten Kodierungen, die bei der Übermittlung der überwachten Telekommunikation verwendet werden.

Daten zur Anzeige des Entgelts, das für die von der zu überwachenden Kennung geführte Telekommunikation anfällt, sind nicht an die berechtigte Stelle zu übermitteln, auch wenn diese Daten an das von der zu überwachenden Kennung genutzte Endgerät übermittelt werden. Auf die wiederholte Übermittlung von Ansagen oder vergleichbaren Daten kann verzichtet werden, solange diese Daten unverändert bleiben.

(2) Der Verpflichtete hat jede bereitgestellte Überwachungskopie und die Daten nach Absatz 1 Satz 1 durch die von der berechtigten Stelle vorgegebene Referenznummer der jeweiligen Überwachungsmaßnahme zu bezeichnen. Der Verpflichtete hat jeden Teil der Überwachungskopie und die zugehörigen Daten nach Absatz 1 Satz 1 zusätzlich durch eine Zuordnungsnummer zu kennzeichnen.

(3) In Fällen, in denen die Überwachungseinrichtungen so gestaltet sind, dass die Kopie des Inhalts der zu überwachenden Telekommunikation getrennt von den durch die Referenznummer gekennzeichneten Daten nach Absatz 1 Satz 1 bereitgestellt werden, sind der berechtigten Stelle ausschließlich diese Daten zu übermitteln, sofern dies im Einzelfall in der Anordnung ausdrücklich bestimmt wird.

(4) Die Absätze 1 bis 3 gelten auch für die Überwachung der Telekommunikation,

1. solange die zu überwachende Kennung an einer Telekommunikation mit mehr als einer Gegenstelle beteiligt ist,

2. wenn unter der zu überwachenden Kennung gleichzeitig mehrere Telekommunikationen stattfinden.

(5) Die Anforderungen nach den Absätzen 1 bis 4 gelten unabhängig von der der jeweiligen Telekommunikationsanlage zu Grunde liegenden Technologie. Die Gestaltung hat der Verpflichtete entsprechend seiner Telekommunikationsanlage festzulegen.

§ 8 Übergabepunkt

(1) Der Verpflichtete hat seine Überwachungseinrichtungen so zu gestalten, dass die Überwachungskopie an einem Übergabepunkt bereitgestellt wird, der den Vorschriften dieser Verordnung und den Vorgaben der Technischen Richtlinie nach § 36 entspricht.

(2) Der Verpflichtete hat den Übergabepunkt so zu gestalten, dass

1. dieser ausschließlich von dem Verpflichteten oder seinem Erfüllungsgehilfen gesteuert werden kann; in Fällen, in denen der Übergabepunkt mittels Fernzugriffs gesteuert werden soll, muss sichergestellt sein, dass der Fernzugriff ausschließlich über die Überwachungseinrichtungen des Verpflichteten erfolgen kann;

2. an diesem ausschließlich die Überwachungskopie bereitgestellt wird;

3. der berechtigten Stelle die Überwachungskopie grundsätzlich in dem Format bereitgestellt wird, in dem dem Verpflichteten die zu überwachende Telekommunikation vorliegt; Absatz 3 Satz 1 und 2 bleibt unberührt;

4. die Qualität der an dem Übergabepunkt bereitgestellten Überwachungskopie grundsätzlich nicht schlechter ist als die der zu überwachenden Telekommunikation;

5. die Überwachungskopie so bereitgestellt wird, dass der Telekommunikationsinhalt grundsätzlich getrennt nach Sende- und Empfangsrichtung des Endgerätes, das für die durch die zu überwachende Kennung bezeichnete Telekommunikation genutzt wird, an die Aufzeichnungsanschlüsse übermittelt wird; dies gilt auch, wenn die zu überwachende Kennung an einer Telekommunikation mit mehr als einer Gegenstelle beteiligt ist;

6. die Zugänge zu dem Telekommunikationsnetz, das für die Übermittlung der Überwachungskopie benutzt wird, Bestandteile des Übergabepunktes sind und

7. hinsichtlich der Fähigkeit zur Übermittlung der Überwachungskopie folgende Anforderungen erfüllt werden:

   a) die Übermittlung der Überwachungskopie an die Aufzeichnungsanschlüsse erfolgt grundsätzlich über geeignete öffentliche Telekommunikationsnetze oder über genormte, allgemein verfügbare Übertragungswege und Übertragungsprotokolle,

   b) die Übermittlung der Überwachungskopie an die Aufzeichnungsanschlüsse wird ausschließlich von den Überwachungseinrichtungen jeweils unmittelbar nach dem Erkennen einer zu überwachenden Telekommunikation eingeleitet und

   c) die Schutzanforderungen gemäß § 14 Absatz 2 werden unterstützt.

   Wird in begründeten Ausnahmefällen bei bestimmten Telekommunikationsanlagen von dem Grundsatz nach Satz 1 Nummer 3 abgewichen, hat der Verpflichtete dies in den der Bundesnetzagentur nach § 19 Absatz 2 einzureichenden Unterlagen darzulegen; die Bundesnetzagentur entscheidet abschließend, ob und für welchen Zeitraum Abweichungen geduldet werden. Auf die Richtungstrennung nach Satz 1 Nummer 5 kann in Fällen verzichtet werden, in denen es sich bei der zu überwachenden Telekommunikation um einseitig gerichtete Telekommunikation oder um nicht vollduplexfähige Telekommunikation handelt.

(3) Wenn der Verpflichtete die ihm zur Übermittlung anvertraute Telekommunikation netzseitig durch technische Maßnahmen gegen unbefugte Kenntnisnahme schützt oder er bei der Erzeugung oder dem Austausch von Schlüsseln mitwirkt und ihm dadurch die Entschlüsselung der Telekommunikation möglich ist, hat er die für diese Telekommunikation angewendeten Schutzvorkehrungen bei der an dem Übergabepunkt bereitzustellenden Überwachungskopie aufzuheben. Satz 1 gilt entsprechend bei der Anwendung von Komprimierungsverfahren. § 14 Absatz 2 bleibt unberührt.

§ 9 Übermittlung der Überwachungskopie

(1) Die Übermittlung der Überwachungskopie einschließlich der Daten nach § 7 Absatz 1 Satz 1 sowie der Referenznummern und Zuordnungsnummern nach § 7 Absatz 2 vom Übergabepunkt an die berechtigte Stelle soll über öffentliche Telekommunikationsnetze erfolgen. Dem Verpflichteten werden hierzu von der berechtigten Stelle für jede zu überwachende Kennung die Aufzeichnungsanschlüsse benannt, an die die Überwachungskopie zu übermitteln ist und die so gestaltet sind, dass sie Überwachungskopien mehrerer gleichzeitig stattfindender zu überwachender Telekommunikationen einer zu überwachenden Kennung entgegennehmen können. Die Rufnummern oder anderen Adressierungsangaben der Aufzeichnungsanschlüsse können voneinander abweichen, wenn die Kopie der zu überwachenden Telekommunikationsinhalte und die zugehörigen Daten nach § 7 Absatz 1 Satz 1 einschließlich der Referenznummern und Zuordnungsnummern nach § 7 Absatz 2 über voneinander getrennte Wege oder über Netze mit unterschiedlicher Technologie übermittelt werden. Die Inanspruchnahme der öffentlichen Telekommunikationsnetze für die Übermittlung der Überwachungskopie ist auf die hierfür erforderliche Zeitdauer zu begrenzen.

(2) (weggefallen)

(3) Maßnahmen zum Schutz der zu übermittelnden Überwachungskopie richten sich nach § 14.

§ 10 Zeitweilige Übermittlungshindernisse

Der Verpflichtete hat seine Überwachungseinrichtungen so zu gestalten, dass die Daten nach § 7 Absatz 1 Satz 1 einschließlich der Referenznummern und Zuordnungsnummern nach § 7 Absatz 2 in Fällen, in denen die Übermittlung der Überwachungskopie an den Aufzeichnungsanschluss ausnahmsweise nicht möglich ist, unverzüglich nachträglich übermittelt werden. Eine Verhinderung oder Verzögerung der zu überwachenden Telekommunikation oder eine Speicherung des Inhalts der Überwachungskopie aus diesen Gründen ist nicht zulässig. Eine für den ungestörten Funktionsablauf aus technischen, insbesondere übermittlungstechnischen Gründen erforderliche Pufferung der Überwachungskopie bleibt von Satz 2 unberührt.

§ 11 (weggefallen)

Abschnitt 3 Organisatorische Anforderungen, Schutzanforderungen

§ 12 Entgegennahme der Anordnung, Rückfragen

(1) Der Verpflichtete hat sicherzustellen, dass er jederzeit telefonisch über das Vorliegen einer Anordnung und die Dringlichkeit ihrer Umsetzung benachrichtigt werden kann. Der Verpflichtete hat sicherzustellen, dass er eine Anordnung innerhalb seiner üblichen Geschäftszeiten jederzeit entgegennehmen kann. Außerhalb seiner üblichen Geschäftszeiten muss er eine unverzügliche Entgegennahme der Anordnung sicherstellen, spätestens jedoch nach sechs Stunden nach der Benachrichtigung. Soweit in der Anordnung eine kürzere Zeitspanne festgelegt ist, sind die dazu erforderlichen Schritte mit der berechtigten Stelle im Einzelfall abzustimmen. Für die Benachrichtigung und für die Entgegennahme der Anordnung hat der Verpflichtete der Bundesnetzagentur eine im Inland gelegene Stelle sowie deren übliche Geschäftszeiten anzugeben; Änderungen sind unverzüglich mitzuteilen. Die Stelle des Verpflichteten muss für die berechtigten Stellen zu dem gewöhnlichen Entgelt für eine einfache Telekommunikationsverbindung erreichbar sein.

(2) Der Verpflichtete hat die zur Umsetzung einer Anordnung erforderlichen Schritte auch auf Grund einer ihm auf gesichertem elektronischem Weg oder vorab per Telefax übermittelten Kopie der Anordnung einzuleiten. Eine auf Grund eines Telefax eingeleitete Überwachungsmaßnahme hat der Verpflichtete wieder abzuschalten, sofern ihm das Original oder eine beglaubigte Abschrift der Anordnung nicht binnen einer Woche nach Übermittlung der Kopie vorgelegt wird. Bei Übermittlung der Anordnung auf gesichertem elektronischen Weg hat der Verpflichtete sicherzustellen, dass

1. die Anordnung und die zugehörigen Daten in seinem Verantwortungsbereich nicht verändert und
2. die für die technische Umsetzung erforderlichen Arbeitsschritte in keinem Fall ohne Mitwirkung seines Personals eingeleitet

werden können.

(3) Der Verpflichtete hat sicherzustellen, dass er telefonische Rückfragen der berechtigten Stellen zur technischen Umsetzung einzelner noch nicht abgeschlossener Überwachungsmaßnahmen jederzeit durch sachkundiges Personal entgegennehmen kann. Ist eine sofortige Klärung nicht möglich, hat der Verpflichtete den Sachverhalt während der üblichen Geschäftszeiten unverzüglich, außerhalb der üblichen Geschäftszeiten innerhalb von sechs Stunden, einer Klärung zuzuführen und die anfragende Stelle über den Sachstand der Klärung zu benachrichtigen. Andere Rechtsvorschriften, nach denen die berechtigten Stellen im Einzelfall eine frühere Beantwortung ihrer Rückfragen fordern können, bleiben unberührt. *4*Für die Angabe und Erreichbarkeit der die Rückfragen entgegennehmenden Stelle des Verpflichteten gilt Absatz 1 Satz 5 entsprechend.

§ 13 Störung und Unterbrechung

Während einer Überwachungsmaßnahme hat der Verpflichtete die betroffenen berechtigten Stellen unverzüglich über Störungen seiner Überwachungseinrichtungen und Unterbrechungen einer Überwachungsmaßnahme zu verständigen. Dabei sind anzugeben:

1. die Art der Störung oder der Grund der Unterbrechung und deren Auswirkungen auf die laufenden Überwachungsmaßnahmen sowie

2. der Beginn und die voraussichtliche Dauer der Störung oder Unterbrechung.

Nach Behebung der Störung oder Beendigung der Unterbrechung sind die betroffenen berechtigten Stellen unverzüglich über den Zeitpunkt zu verständigen, ab dem die Überwachungseinrichtungen wieder ordnungsgemäß zur Verfügung stehen. Der Verpflichtete hat seine Überwachungseinrichtungen unverzüglich und vorrangig vor Telekommunikationsanschlüssen anderer Teilnehmer zu entstören. In Mobilfunknetzen sind die Angaben über Störungen, die sich nur in regional begrenzten Bereichen des Netzes auswirken, nur auf Nachfrage der berechtigten Stelle zu machen.

§ 14 Schutzanforderungen

(1) Der Verpflichtete hat die von ihm zu treffenden Vorkehrungen zur technischen und organisatorischen Umsetzung von Anordnungen, insbesondere die technischen Einrichtungen zur Steuerung der Überwachungsfunktionen und des Übergabepunktes nach § 8 einschließlich der zwischen diesen befindlichen Übertragungsstrecken, nach dem Stand der Technik gegen unbefugte Inanspruchnahme zu schützen; die technischen Einrichtungen zur Steuerung der Überwachungsfunktionen und des Übergabepunktes nach § 8 sind im Inland zu betreiben.

(2) Die Überwachungskopie ist durch angemessene Verfahren gegen eine Kenntnisnahme durch unbefugte Dritte zu schützen. Für die Übermittlung der Überwachungskopie an die Aufzeichnungsanschlüsse, die durch angemessene technische Maßnahmen vor einer unbefugten Belegung geschützt sind, sind Verfahren anzuwenden, die einen angemessenen Schutz vor einer Übermittlung an Nichtberechtigte gewährleisten. Die zur Erreichung der Ziele nach den Sätzen 1 und 2 erforderlichen Verfahren sind in der Technischen Richtlinie nach § 36 festzulegen. Sollen die Schutzziele nach Satz 2 im Rahmen einer Geschlossenen Benutzergruppe erreicht werden, darf hierfür ausschließlich eine eigens für diesen Zweck eingerichtete Geschlossene Benutzergruppe genutzt werden, die durch die Bundesnetzagentur verwaltet wird. Die Schutzanforderung nach Satz 1 gilt bei der Übermittlung der Überwachungskopie an die Aufzeichnungsanschlüsse über festgeschaltete Übertragungswege oder über Telekommunikationsnetze mit leitungsvermittelnder Technik auf Grund der diesen Übertragungsmedien zu Grunde liegenden Gestaltungsgrundsätze als erfüllt. In

den übrigen Fällen sind die zur Erfüllung dieser Schutzanforderung erforderlichen technischen Schutzvorkehrungen auf der Seite der Telekommunikationsanlage des Verpflichteten Bestandteil der Überwachungseinrichtungen und auf der Seite der berechtigten Stelle Bestandteil der Aufzeichnungs- und Auswertungseinrichtungen.

(3) Im Übrigen erfolgt die Umsetzung von Anordnungen unter Beachtung der beim Betreiben von Telekommunikationsanlagen oder Erbringen von Telekommunikationsdiensten üblichen Sorgfalt. Dies gilt insbesondere hinsichtlich der Sicherheit und Verfügbarkeit zentralisierter oder teilzentralisierter Einrichtungen, sofern Überwachungsmaßnahmen mittels solcher Einrichtungen eingerichtet und verwaltet werden. Die Verpflichteten haben dafür zu sorgen, dass die mit der Umsetzung von Überwachungsmaßnahmen betrauten Personen die damit zusammenhängenden Tätigkeiten nur in sich beim Verpflichteten oder dessen Erfüllungsgehilfen befindlichen Räumen ausführen, in denen Unbefugte keine Kenntnis von der Anordnung oder den darauf beruhenden Tätigkeiten erhalten können. Satz 3 gilt nicht für die Entgegennahme der Benachrichtigung über das Vorliegen einer Anordnung gemäß § 12 Absatz 1 Satz 1.

§ 15 Verschwiegenheit

(1) Der Verpflichtete darf Informationen über die Art und Weise, wie Anordnungen in seiner Telekommunikationsanlage umgesetzt werden, Unbefugten nicht zugänglich machen.

(2) Der Verpflichtete hat den Schutz der im Zusammenhang mit Überwachungsmaßnahmen stehenden Informationen sicherzustellen. Dies gilt insbesondere hinsichtlich unbefugter Kenntnisnahme von Informationen über zu überwachende Kennungen und die Anzahl gegenwärtig oder in der Vergangenheit überwachter Kennungen sowie die Zeiträume, in denen Überwachungsmaßnahmen durchgeführt worden sind. Für unternehmensinterne Prüfungen, die in keinem unmittelbaren Zusammenhang mit der Umsetzung von Anordnungen stehen, darf jedoch die Anzahl der in einem zurückliegenden Zeitraum betroffenen zu überwachenden Kennungen mitgeteilt werden, sofern sichergestellt ist, dass keine Rückschlüsse auf die betroffenen Kennungen oder auf die die Überwachung durchführenden Stellen möglich sind.

(3) In Fällen, in denen dem Verpflichteten bekannt wird oder er einen begründeten Verdacht hat, dass ein Unbefugter entgegen Absatz 2 Kenntnis von einer Überwachungsmaßnahme erlangt hat, hat der Verpflichtete die betroffene berechtigte Stelle und die Bundesnetzagentur unverzüglich und umfassend über das Vorkommnis zu informieren.

§ 16 Protokollierung

(1) Der Verpflichtete hat sicherzustellen, dass jede Anwendung seiner Überwachungseinrichtungen, die als integraler Bestandteil der Telekommunikationsanlage gestaltet sind, bei der Eingabe der für die technische Umsetzung erforderlichen Daten automatisch lückenlos protokolliert wird. Unter Satz 1 fallen auch Anwendungen für unternehmensinterne Testzwecke, für Zwecke des Nachweises (§ 19 Absatz 5), für Prüfungen im Falle von Änderungen der Telekommunikationsanlage oder nachträglich festgestellten Mängeln (§ 20) und für probeweise Anwendungen der Überwachungsfunktionen (§ 23) sowie solche Anwendungen, die durch fehlerhafte oder missbräuchliche Eingabe, Bedienung oder Schaltung verursacht wurden. Es sind zu protokollieren:

1. die Referenznummer oder eine unternehmensinterne Bezeichnung der Überwachungsmaßnahme,

2. die tatsächlich eingegebene Kennung, auf Grund derer die Überwachungseinrichtungen die Überwachungskopie bereitstellen,

3. die Zeitpunkte (Datum und Uhrzeit auf der Grundlage der amtlichen Zeit), zwischen denen die Überwachungseinrichtungen die Telekommunikation in Bezug auf die Kennung nach Nummer 2 erfassen,

4. die Rufnummer oder andere Adressierungsangabe des Anschlusses, an den die Überwachungskopie übermittelt wird,

5. ein Merkmal zur Erkennbarkeit der Person, die die Daten nach den Nummern 1 bis 4 eingibt,

6. Datum und Uhrzeit der Eingabe.

Die Angaben nach Satz 3 Nummer 5 dürfen ausschließlich bei auf tatsächlichen Anhaltspunkten beruhenden Untersuchungen zur Aufklärung von Missbrauchs- oder Fehlerfällen verwendet werden.

(2) Der Verpflichtete hat sicherzustellen, dass durch die technische Gestaltung der Zugriffsrechte und Löschfunktionen folgende Anforderungen eingehalten werden:

1. das Personal, das mit der technischen Umsetzung von Anordnungen betraut ist, darf keinen Zugriff auf die Protokolldaten, die Löschfunktionen und die Funktionen zur Erteilung von Zugriffsrechten haben;

2. die Funktionen zur Löschung von Protokolldaten dürfen ausschließlich dem für die Prüfung dieser Daten verantwortlichen Personal des Verpflichteten verfügbar sein;

3. jede Nutzung der Löschfunktionen nach Nummer 2 ist unter Angabe des Zeitpunktes und eines Merkmals zur Erkennbarkeit der die Funktion jeweils nutzenden Person in einem

Datensatz zu protokollieren, der frühestens nach zwei Jahren gelöscht oder überschrieben werden darf;

4. die Berechtigungen zum Zugriff auf die Funktionen von Datenverarbeitungsanlagen oder auf die Datenbestände, die für die Prüfung der Protokolldaten oder die Erteilung von Zugriffsrechten erforderlich sind, dürfen nicht ohne Nachweis eingerichtet, geändert oder gelöscht werden können; jede Erteilung, Änderung oder Aufhebung einer Berechtigung ist einschließlich ihres Zeitpunktes bis zum Ende des zweiten auf die Erteilung, Änderung oder Aufhebung folgenden Kalenderjahres so zu dokumentieren, dass die Daten, einschließlich aller bestehenden Berechtigungen, im Rahmen der üblichen Geschäftszeiten jederzeit für Prüfungen abrufbar sind.

§ 17 Prüfung und Löschung der Protokolldaten, Vernichtung von Unterlagen

(1) Der Verpflichtete hat einen angemessenen Anteil der für die Aktivierung, Änderung oder Abschaltung der Überwachungsfunktionalität nach § 16 protokollierten Eingaben auf Übereinstimmung mit den ihm vorliegenden Unterlagen zu prüfen. Die Prüfung hat mindestens quartalsweise zu erfolgen, die unternehmensinterne Festlegung kürzerer Prüfzeiträume ist zulässig. Die Überprüfung muss sich auf mindestens 20 vom Hundert der im Prüfzeitraum angeordneten Überwachungsmaßnahmen beziehen, jedoch nicht mehr als 200 Maßnahmen je Kalendervierteljahr umfassen. Darüber hinaus sind die Protokolldaten in allen Fällen zu prüfen,

1. die in § 23 genannt sind, oder
2. in denen Tatsachen den Verdacht einer Unregelmäßigkeit begründen.

In den geheimschutzbetreuten Unternehmen obliegen die Aufgaben nach den Sätzen 1 und 4 dem Sicherheitsbevollmächtigten. Das mit der Prüfung betraute Personal kann zur Klärung von Zweifelsfällen das mit der technischen Umsetzung der Anordnungen betraute Personal hinzuziehen. Der Verpflichtete hat die Ergebnisse der Prüfungen schriftlich festzuhalten. Sind keine Beanstandungen aufgetreten, darf in den Prüfergebnissen die nach § 16 Absatz 1 Satz 3 Nummer 2 protokollierte Kennung nicht mehr vermerkt sein und kann auf die übrigen Angaben gemäß § 16 Absatz 1 Satz 3 verzichtet werden. Der Verpflichtete hat der Bundesnetzagentur spätestens zum Ende eines jeden Kalendervierteljahres eine Kopie der Prüfergebnisse zu übersenden. Die Bundesnetzagentur bewahrt diese Unterlagen bis zum Ende des folgenden Kalenderjahres auf; sie kann sie bei der Einsichtnahme nach Absatz 4 verwenden.

(2) Der Verpflichtete hat die Protokolldaten vorbehaltlich Satz 2 und Absatz 3 Satz 6 nach Ablauf von zwölf Monaten nach Versendung der Prüfergebnisse an die Bundesnetzagentur unverzüglich zu löschen und die entsprechenden Anordnungen und alle zugehörigen

Unterlagen einschließlich der für die jeweilige Überwachungsmaßnahme angefertigten unternehmensinternen Hilfsmittel zu vernichten, es sei denn, dass die Überwachungsmaßnahme zu diesem Zeitpunkt noch nicht beendet ist. Andere Rechtsvorschriften, die eine über Satz 1 hinausgehende Aufbewahrungszeit für Unterlagen vorschreiben, bleiben unberührt; dies gilt entsprechend auch für unternehmensinterne Vorgaben zur Aufbewahrung von Abrechnungsunterlagen.

(3) Bei Beanstandungen, insbesondere auf Grund unzulässiger Eingaben oder unzureichender Angaben, hat der Verpflichtete unverzüglich eine Untersuchung der Angelegenheit einzuleiten und die Bundesnetzagentur unter Angabe der wesentlichen Einzelheiten schriftlich darüber zu unterrichten. Steht die Beanstandung im Zusammenhang mit einer Überwachungsmaßnahme, hat der Verpflichtete zusätzlich unverzüglich die betroffene berechtigte Stelle zu informieren. Die Pflicht zur Untersuchung und Unterrichtung nach den Sätzen 1 und 2 besteht auch für Fälle, in denen der Verpflichtete unabhängig von der Prüfung der Protokolldaten Kenntnis über einen zu beanstandenden Sachverhalt erhält. Das Ergebnis der Untersuchung ist schriftlich festzuhalten. Der Verpflichtete hat eine Kopie des Untersuchungsergebnisses an die Bundesnetzagentur zu übersenden, die sie bis zum Ende des folgenden Kalenderjahres aufbewahrt. Für die Löschung der beanstandeten Protokolldaten und die Vernichtung der zugehörigen Unterlagen nach Abschluss der gemäß Satz 1 oder Satz 3 durchzuführenden Untersuchungen gilt Absatz 2 vorbehaltlich anderer Rechtsvorschriften entsprechend mit der Maßgabe, dass an die Stelle des dort genannten Zeitpunktes der Dezember des Kalenderjahres tritt, das auf den Abschluss der Untersuchung folgt.

(4) Die Bundesnetzagentur ist befugt, Einsicht in die Protokolldaten, Anordnungen und die zugehörigen Unterlagen sowie in die Datensätze nach § 16 Absatz 2 Nummer 3 und 4 zu nehmen. Die Befugnisse der für die Kontrolle der Einhaltung der Vorschriften über den Schutz personenbezogener Daten zuständigen Behörden werden durch die Absätze 1 bis 3 nicht berührt. Für die gemäß § 16 erstellten Protokolldaten muss für die Kontrollen nach den Sätzen 1 und 2 die Möglichkeit bestehen, diese sowohl nach ihrer Entstehungszeit als auch nach den betroffenen Kennungen sortiert auszugeben.

Abschnitt 4 Verfahren zum Nachweis nach § 110 Absatz 1 Satz 1 Nummer 3 des Telekommunikationsgesetzes

§ 18 (weggefallen)

§ 19 Nachweis

(1) Für den nach § 110 Absatz 1 Satz 1 Nummer 3 des Telekommunikationsgesetzes zu erbringenden Nachweis der Übereinstimmung der von dem Verpflichteten getroffenen Vorkehrungen mit den Vorschriften dieser Verordnung und der Technischen Richtlinie (§ 36)

hat der Verpflichtete der Bundesnetzagentur die zur Prüfung erforderlichen Unterlagen einzureichen und ihr die erforderlichen Prüfungen der Überwachungseinrichtungen und der organisatorischen Vorkehrungen vor Ort zu ermöglichen. Den Nachweis für baugleiche Einrichtungen hat der Verpflichtete nur einmal zu erbringen; die Bundesnetzagentur kann jedoch in begründeten Fällen einen weiteren Nachweis an einer baugleichen Einrichtung verlangen.

(2) Die von dem Verpflichteten vorzulegenden Unterlagen, zu deren Form die Bundesnetzagentur Vorgaben machen kann, müssen die zur Beurteilung des Sachverhalts erforderlichen Angaben enthalten. Dazu gehören insbesondere Angaben zu Name und Sitz des Verpflichteten sowie die Namen der Personen, die für die Vorhaltung der Überwachungseinrichtungen verantwortlich sind, sowie Beschreibungen über:

1. die technische Gestaltung der Telekommunikationsanlage einschließlich der mit ihr erbrachten oder geplanten Telekommunikationsdienste und der zugehörigen Dienstmerkmale,

2. die Arten der Kennungen, die bei den erbrachten oder geplanten Telekommunikationsdiensten ausgewertet werden können,

3. die Überwachungseinrichtungen, insbesondere hinsichtlich der Anforderungen nach § 7 Absatz 1 bis 4 sowie § 10,

4. den Übergabepunkt gemäß § 8 und die Bereitstellung der Überwachungskopie gemäß § 9 sowie

5. die technischen Einrichtungen und die organisatorischen Vorkehrungen zur Umsetzung der §§ 4, 5, 6, 12 und 13 Satz 4, des § 14 Absatz 1, 2 Satz 1 bis 4 und Absatz 3 sowie der §§ 16 und 17 Absatz 1 Satz 1 bis 4 sowie

6. die technische Gestaltung des Zusammenwirkens der Überwachungseinrichtungen mit den Telekommunikationsanlagen anderer Betreiber.

Unterlagen, die Geschäfts- oder Betriebsgeheimnisse enthalten, sind entsprechend zu kennzeichnen. Soweit für die Überwachungseinrichtungen auf Antrag des Herstellers oder Vertreibers dieser Einrichtungen eine Typmusterprüfung nach § 110 Absatz 4 des Telekommunikationsgesetzes durchgeführt wurde, kann der Verpflichtete zur Vereinfachung auf die Ergebnisse dieser Typmusterprüfung verweisen.

(3) Die Bundesnetzagentur bestätigt dem Verpflichteten den Eingang der Unterlagen. Sie prüft die Unterlagen darauf, ob die Überwachungseinrichtungen und die organisatorischen Vorkehrungen den Anforderungen der §§ 4, 5, 6 und 7 Absatz 1 bis 4, der §§ 8 bis 10, 12 und 13 Satz 4, des § 14 Absatz 1, 2 Satz 1 bis 4 und Absatz 3, der §§ 16 und 17 Absatz 1 Satz 1 bis 4 sowie den Anforderungen der Technischen Richtlinie nach § 36 entsprechen; dabei berücksichtigt sie die

Zulässigkeit von älteren technischen Vorschriften nach § 36 Satz 4 und von Abweichungen gemäß § 22. Nach Prüfung der schriftlichen Unterlagen vereinbart die Bundesnetzagentur mit dem Verpflichteten einen Termin für eine technische Prüfung der Überwachungseinrichtungen und eine Prüfung der organisatorischen Vorkehrungen.

(4) Die Bundesnetzagentur stellt die prüffähigen Unterlagen unverzüglich dem Generalbundesanwalt beim Bundesgerichtshof, dem Zollkriminalamt, dem Bundesamt für Verfassungsschutz als Koordinierungsstelle für die Nachrichtendienste und dem Bundeskriminalamt als Zentralstelle zur Stellungnahme innerhalb einer gesetzten angemessenen Frist zur Verfügung. Die rechtzeitig eingegangenen Stellungnahmen hat die Bundesnetzagentur bei ihrer Entscheidung über die vorübergehende Duldung von Abweichungen mit zu berücksichtigen.

(5) Die Bundesnetzagentur kann von dem Verpflichteten verlangen, dass er unentgeltlich

1. ihren Bediensteten die Durchführung der erforderlichen Prüfungen bezüglich der Einhaltung der in Absatz 3 genannten Anforderungen ermöglicht,

2. bei Prüfungen nach Nummer 1 im erforderlichen Umfang mitwirkt und

3. die für die Prüfungen nach Nummer 1 erforderlichen Telekommunikationsanschlüsse seiner Telekommunikationsanlage sowie die notwendigen Endgeräte bereitstellt und die für die Prüfung notwendige Telekommunikation an geeignete Testanschlüsse übermittelt.

Für die Zwecke der Prüfung der Protokolldaten nach § 17 bestätigt die Bundesnetzagentur dem Verpflichteten den Zeitraum der Prüfung, die Kennungen der für die Prüfung verwendeten Telekommunikationsanschlüsse sowie die Rufnummern oder anderen Adressierungsangaben der Anschlüsse, an die die Kopie der Telekommunikation übermittelt wurde. Die Bundesnetzagentur kann zu den Prüfungen nach Satz 1 auch Vertreter der in Absatz 4 genannten Stellen hinzuziehen. Für Prüfungen, die die Bundesnetzagentur nach § 110 Absatz 1 Satz 1 Nummer 4 des Telekommunikationsgesetzes im Falle von nachträglich aufgetretenen Mängeln durchführt, gelten die Sätze 1 bis 3 entsprechend.

(6) Entsprechen die von dem Verpflichteten vorgehaltenen Überwachungseinrichtungen und die von ihm getroffenen organisatorischen Vorkehrungen den Vorschriften dieser Verordnung und der Technischen Richtlinie nach § 36, erteilt die Bundesnetzagentur dem Verpflichteten innerhalb von vier Wochen nach Abschluss der Prüfungen nach Absatz 5 einen entsprechenden Nachweisbescheid. Weichen die vorgehaltenen Überwachungseinrichtungen oder die getroffenen organisatorischen Vorkehrungen von den Vorschriften ab, hat die Bundesnetzagentur dem Verpflichteten aufzuerlegen, die Abweichung innerhalb einer angemessenen Frist zu beseitigen. Eine dauerhafte Abweichung kann nur geduldet werden, wenn zu erwarten ist, dass die Durchführung von Überwachungsmaßnahmen nicht beeinträchtigt wird und keine Änderungen bei den Aufzeichnungs- und Auswertungs-

einrichtungen erforderlich sind; in diesem Fall sind die geduldeten Abweichungen im Nachweisbescheid zu bezeichnen. Bei Abweichungen, die eine Verletzung des Fernmeldegeheimnisses oder wesentliche Mängel bei der Überwachung zur Folge haben, hat die Bundesnetzagentur in dem Nachweisbescheid darzustellen, dass der Nachweis für diejenigen Dienste oder Dienstmerkmale nicht erbracht ist, bei denen sich diese Abweichungen auswirken.

(7) Gehen die Unterlagen nach Absatz 2 erst so spät bei der Bundesnetzagentur ein, dass von ihr angeforderte Ergänzungen nicht mehr fristgerecht erfolgen können, soll sie vor Einleiten von Zwangsmitteln nach § 115 Absatz 2 oder 3 des Telekommunikationsgesetzes eine Nachbesserungsfrist einräumen, die einen Monat nicht übersteigen darf.

(8) Im Falle der Fortschreibung der Unterlagen, insbesondere im Zusammenhang mit Änderungen wie nach § 20, hat der Verpflichtete der Bundesnetzagentur entsprechend geänderte Unterlagen zusammen mit einer Liste der jeweils insgesamt gültigen Dokumente vorzulegen; die Absätze 1 bis 7 gelten entsprechend.

§ 20 Änderungen der Telekommunikationsanlage oder der Überwachungseinrichtung

§ 19 gilt entsprechend bei jeder Änderung der Telekommunikationsanlage, eines mittels dieser Telekommunikationsanlage angebotenen Telekommunikationsdienstes oder der Überwachungseinrichtung, sofern diese Änderung Einfluss auf die Überwachungsfunktionen hat. Änderungen, die Auswirkungen auf die Aufzeichnungs- oder Auswertungseinrichtungen haben, dürfen erst nach Abstimmung mit der Bundesnetzagentur vorgenommen werden.

Abschnitt 5 Abweichungen

§ 21 (weggefallen)

§ 22 Abweichungen, Feldversuche, Probebetriebe

(1) Die Bundesnetzagentur kann im Rahmen des Nachweises nach § 19 im Benehmen mit den in § 19 Absatz 4 genannten Stellen auf Antrag des Verpflichteten bei einzelnen Telekommunikationsanlagen hinsichtlich der Gestaltung der Überwachungseinrichtungen Abweichungen von einzelnen Anforderungen der Technischen Richtlinie nach § 36 dulden, sofern

1. die Überwachbarkeit sichergestellt ist und die Durchführung von Überwachungsmaßnahmen nicht grundlegend beeinträchtigt wird und

2. ein hierdurch bedingter Änderungsbedarf bei den Aufzeichnungs- und Auswertungseinrichtungen nicht unverhältnismäßig hoch ist.

Der Verpflichtete hat der Bundesnetzagentur die Gründe für Abweichungen nach Satz 1, die genaue Beschreibung des Übergabepunktes mit Hinweisen auf die Abweichungen von den Vorschriften sowie die Folgen dieser Abweichungen mitzuteilen. Die Bundesnetzagentur ist unbeschadet möglicher Schutzrechtsvermerke des Verpflichteten befugt, Mitteilungen nach Satz 2 an die in § 19 Absatz 4 genannten Stellen zu übermitteln, damit die vorhandenen Aufzeichnungs- und Auswertungseinrichtungen gegebenenfalls angepasst werden können. Der Nachweisbescheid kann mit Auflagen verbunden werden. *5*In der Technischen Richtlinie nach § 36 können für bestimmte Telekommunikationsanlagen oder Telekommunikationsdienste technische Voraussetzungen festgelegt werden, bei deren Einhaltung Abweichungen allgemein zulässig sind.

(2) Die Bundesnetzagentur kann für die Überwachungseinrichtungen in Teilen von Telekommunikationsanlagen, die Versuchs- oder Probezwecken oder im Rahmen von Feldversuchen der Ermittlung der Funktionsfähigkeit der Telekommunikationsanlage unter tatsächlichen Betriebsbedingungen oder der bedarfsgerechten Ausgestaltung von am Telekommunikationsmarkt nachgefragten Telekommunikationsdiensten dienen, den Nachweis im Hinblick auf den befristet betriebenen Teil der Telekommunikationsanlage oder den befristet oder einem begrenzten Teilnehmerkreis angebotenen Telekommunikationsdienst nach einem vereinfachten Verfahren annehmen; Wiederholungen sind zulässig. Sie kann dabei nach pflichtgemäßem Ermessen im Einzelfall vorübergehend auf die Einhaltung einzelner technischer Vorschriften dieser Verordnung oder einzelner Anforderungen der Technischen Richtlinie nach § 36 verzichten, sofern

1. der Versuchs- oder Probebetrieb oder der Feldversuch des Teils der Telekommunikationsanlage für nicht länger als zwölf Monate vorgesehen ist,

2. nicht mehr als 10 000 Teilnehmer oder sonstige Nutzungsberechtigte, die nicht zu dem Personal des Verpflichteten zählen, in den Versuchs- oder Probebetrieb oder in den Feldversuch einbezogen werden und

3. sichergestellt ist, dass eine Überwachung der Telekommunikation möglich ist.

Absatz 1 Satz 2 bis 4 gilt entsprechend.

Abschnitt 6 Sonstige Vorschriften

§ 23 Probeweise Anwendung der Überwachungsfunktionen

(1) Die probeweise Anwendung der Überwachungsfunktionen ist auf das unabdingbare Maß zu begrenzen und nur zulässig

1. zur Durchführung des Nachweises nach § 19 oder einer im Einzelfall von der Bundesnetzagentur verlangten Prüfung nach § 110 Absatz 1 Satz 1 Nummer 4 des Telekommunikationsgesetzes,

2. zur Funktionsprüfung der Überwachungseinrichtungen durch den Betreiber oder zur Schulung von Personal des Verpflichteten unter Verwendung von ausschließlich zu diesem Zweck eingerichteten Anschlüssen oder

3. zur Funktionsprüfung der Aufzeichnungs- und Auswertungseinrichtungen; Aus- oder Fortbildungsmaßnahmen der berechtigten Stellen stehen solchen Funktionsprüfungen gleich.

Für eine im Einzelfall von der Bundesnetzagentur verlangte Prüfung nach § 110 Absatz 1 Satz 1 Nummer 4 des Telekommunikationsgesetzes kann sie vom Verpflichteten auch verlangen, dass für automatisch durchzuführende Prüfungen gleichzeitig mehrere Testanschlüsse und Endgeräte bereitgestellt werden sowie eine von der Bundesnetzagentur bereitgestellte Anwendung auf diesen Endgeräten installiert wird. Bei der probeweisen Anwendung ist sicherzustellen, dass die Anschlüsse, auf die die Überwachungsfunktionen angewendet werden, ausschließlich zu Prüfzwecken genutzt werden und die Personen, die für die probeweise erzeugte Telekommunikation verantwortlich sind, diese ohne Beteiligung Dritter durchführen. Der Zeitraum der probeweisen Anwendung nach Satz 1 Nummer 3 darf sechs Monate nicht überschreiten; Verlängerungen sind zulässig. Der Verpflichtete hat der Bundesnetzagentur die von ihm für die Fälle nach Satz 1 Nummer 2 vorgesehenen Anschlüsse vor der erstmaligen Durchführung von Funktionsprüfungen seiner Überwachungseinrichtungen schriftlich anzuzeigen. Die Bundesnetzagentur führt über diese Anschlüsse eine Liste und bestätigt dem Verpflichteten den Eintrag der von ihm benannten Anschlüsse. Nach Eingang dieser Bestätigung kann der Verpflichtete Funktionsprüfungen unter ausschließlicher Einbeziehung dieser Anschlüsse jederzeit eigenverantwortlich nach Bedarf durchführen. In den Fällen des Satzes 1 Nummer 3 bedarf die probeweise Anwendung der vorherigen Anmeldung durch die berechtigte Stelle bei der Bundesnetzagentur. In der Anmeldung sind der Grund für die probeweise Anwendung, der Zeitraum der Erprobung, die Kennungen, die bei der Erprobung an Stelle einer zu überwachenden Kennung verwendet werden, sowie die Rufnummern oder anderen Adressierungsangaben der Anschlüsse anzugeben, an die die Kopie der Telekommunikation übermittelt wird. Die Bundesnetzagentur bestätigt die Anmeldung mit den in Satz 8 genannten Angaben schriftlich oder durch eine gesicherte elektronische Übermittlung sowohl der berechtigten Stelle als auch dem Verpflichteten. In Fällen einer dringenden Störungsbeseitigung ist eine nachträgliche Anzeige oder Anmeldung zulässig. Für die Behandlung der Bestätigung beim Verpflichteten gilt § 17 entsprechend. Form und Übermittlungsverfahren für die Anzeige, die Anmeldung und die Bestätigung sowie Vorgaben für die in diesen Fällen zu verwendende Referenznummer können in der Technischen Richtlinie nach § 36 festgelegt werden.

(2) Zur Durchführung der in Absatz 1 Satz 1 Nummer 3 genannten Aufgaben hat der Verpflichtete der berechtigten Stelle auf Verlangen Telekommunikationsanschlüsse seiner Telekommunikationsanlage zu den üblichen Geschäftsbedingungen an den von dieser benannten Orten einzurichten und zu überlassen und Telekommunikationsdienste bereitzustellen sowie die Überwachungsfunktion bei diesen Anschlüssen nach den zeitlichen Vorgaben der berechtigten Stelle einzurichten.

§ 24 Anforderungen an Aufzeichnungsanschlüsse

(1) Der nach § 110 Absatz 6 des Telekommunikationsgesetzes verpflichtete Betreiber hat der berechtigten Stelle auf Antrag die von ihr benötigten Aufzeichnungsanschlüsse unverzüglich und in dringenden Fällen vorrangig bereitzustellen. *2*Zur Sicherstellung der Erreichbarkeit dieser Anschlüsse und zum Schutz vor falschen Übermittlungen sind geeignete technische Maßnahmen gemäß § 14 Absatz 2 vorzusehen.

(2) Der nach § 110 Absatz 6 des Telekommunikationsgesetzes verpflichtete Betreiber hat im Störungsfall die unverzügliche und vorrangige Entstörung der Anschlüsse nach Absatz 1 sicherzustellen.

§ 25 (weggefallen)

Teil 3

Maßnahmen nach den §§ 5 und 8 des Artikel 10-Gesetzes und den §§ 6, 12 und 14 des BND-Gesetzes

§ 26 Kreis der Verpflichteten

(1) Die Vorschriften dieses Teils gelten für Betreiber von Telekommunikationsanlagen, die

1. der Bereitstellung von internationalen leitungsgebundenen Telekommunikationsbeziehungen dienen, soweit eine gebündelte Übertragung erfolgt oder
2. der Bereitstellung von internationalen Telekommunikationsbeziehungen dienen, über die Telekommunikation von Ausländern im Ausland erfolgt und

für öffentlich zugängliche Telekommunikationsdienste genutzt werden.

(2) Die Bundesnetzagentur kann im Einvernehmen mit dem Bundesnachrichtendienst Betreiber nach Absatz 1 auf deren Antrag für einen bestimmten Zeitraum, der drei Jahre nicht übersteigen darf, von den Verpflichtungen befreien, die sich aus den §§ 27 und 28 ergeben; wiederholte Befreiungen sind zulässig. Für die rechtzeitige Antragstellung gilt die in § 110

Absatz 1 Satz 1 Nummer 3 Halbsatz 2 des Telekommunikationsgesetzes genannte Frist entsprechend. Anträge auf eine wiederholte Befreiung kann der Verpflichtete frühestens drei Monate und spätestens sechs Wochen vor Ablauf der laufenden Frist stellen. Die Bundesnetzagentur soll über die Anträge innerhalb von sechs Wochen entscheiden. Im Falle einer Beendigung der Befreiung hat der Verpflichtete die nach den §§ 27 und 28 erforderlichen technischen und organisatorischen Vorkehrungen innerhalb von sechs Monaten nach Ablauf der bisherigen Befreiungsfrist zu treffen.

§ 27 Grundsätze, technische und organisatorische Umsetzung von Anordnungen, Verschwiegenheit

(1) Die zu überwachende Telekommunikation umfasst bei Überwachungsmaßnahmen nach § 5 oder § 8 des Artikel 10-Gesetzes die Telekommunikation, die auf dem in der Anordnung bezeichneten Übertragungsweg übertragen wird, einschließlich der auf diesem Übertragungsweg übermittelten, für den Auf- oder Abbau von Telekommunikationsverbindungen notwendigen vermittlungstechnischen Steuerzeichen und bei Überwachungsmaßnahmen nach den §§ 6, 12 oder 14 des BND-Gesetzes die Telekommunikation, die in dem in der Anordnung bezeichneten Telekommunikationsnetz übermittelt wird, einschließlich der in diesem Telekommunikationsnetz übermittelten, für den Auf- oder Abbau von Telekommunikationsverbindungen notwendigen vermittlungstechnischen Steuerzeichen. § 5 gilt mit Ausnahme von seinem Absatz 1, 2 Satz 3 und Absatz 4 Satz 2 entsprechend.

(2) Der Verpflichtete hat dem Bundesnachrichtendienst an einem Übergabepunkt im Inland eine vollständige Kopie der Telekommunikation bereitzustellen, die über die in der Anordnung bezeichneten Übertragungswege oder Telekommunikationsnetze übertragen wird.

(3) Der Verpflichtete hat in seinen Räumen die Aufstellung und den Betrieb von Geräten des Bundesnachrichtendienstes zu dulden, die nur von hierzu besonders ermächtigten Bediensteten des Bundesnachrichtendienstes eingestellt und gewartet werden dürfen und die folgende Anforderungen erfüllen:

1. die nach Absatz 2 bereitgestellte Kopie wird bei Überwachungsmaßnahmen nach den §§ 5 oder 8 des Artikel 10-Gesetzes in der Weise bearbeitet, dass die Festlegung nach § 10 Absatz 4 Satz 3 des Artikel 10Gesetzes eingehalten und die danach verbleibende Kopie an den Bundesnachrichtendienst nur insoweit übermittelt wird, als sie Telekommunikation mit dem in der Anordnung nach § 10 Absatz 4 Satz 2 des Artikel 10-Gesetzes bezeichneten Gebiet enthält; im Übrigen wird die Kopie gelöscht;

2. ein unbefugter Fernzugriff auf die Geräte ist ausgeschlossen;

3. die Geräte verfügen über eine dem Stand der Technik entsprechende Zugriffskontrolle und über eine automatische lückenlose Protokollierung aller Zugriffe;

4. die Einhaltung der Anforderungen nach den Nummern 1 bis 3 ist durch das Bundesamt für Sicherheit in der Informationstechnik zertifiziert.

(4) Der Verpflichtete hat während seiner üblichen Geschäftszeiten folgenden Personen nach Anmeldung Zutritt zu den in Absatz 3 bezeichneten Geräten zu gewähren:

1. den Bediensteten des Bundesnachrichtendienstes zur Einstellung und Wartung der Geräte,

2. bei Überwachungsmaßnahmen nach den §§ 5 oder 8 des Artikel 10-Gesetzes zusätzlich den Mitgliedern und Mitarbeitern der G 10-Kommission (§ 1 Absatz 2 des Artikel 10-Gesetzes) zur Kontrolle der Geräte und ihrer Datenverarbeitungsprogramme sowie der Protokolle nach Absatz 3 Nummer 3.

Der Verpflichtete hat sicherzustellen, dass eine unbeaufsichtigte Tätigkeit der nach Satz 1 Zutrittsberechtigten auf die in Absatz 3 bezeichneten Geräte begrenzt bleibt.

(5) Im Einzelfall erforderlich werdende ergänzende Einzelheiten hinsichtlich der Aufstellung der in Absatz 3 bezeichneten Geräte und des Zugangs zu diesen Geräten sind in einer Vereinbarung zwischen dem Verpflichteten und dem Bundesnachrichtendienst zu regeln.

(6) Der Verpflichtete hat seine Überwachungseinrichtungen so zu gestalten und die organisatorischen Vorkehrungen so zu treffen, dass er eine Anordnung unverzüglich umsetzen kann.

(7) Für die Gestaltung des Übergabepunktes gilt § 8 Absatz 2 Satz 1 Nummer 1 bis 4 entsprechend. Technische Einzelheiten zum Übergabepunkt können in der Technischen Richtlinie nach § 36 festgelegt werden, sie können jedoch auch in Abstimmung mit der Bundesnetzagentur und den betroffenen Interessenvertretern festgelegt werden.

(8) Für die Entstörung und Störungsmeldung, für die Schutzanforderungen, für die Pflicht zur Verschwiegenheit, für die Entgegennahme der Information über das Vorliegen einer Anordnung und die Entgegennahme einer Anordnung sowie für Rückfragen gelten § 12 Absatz 1 Satz 5 und Absatz 3, §§ 13, 14 Absatz 1 und 3 sowie § 15 entsprechend mit der von § 12 Absatz 1 Satz 1 bis 3 und Absatz 3 Satz 1 abweichenden Maßgabe, dass der Verpflichtete innerhalb seiner üblichen Geschäftszeiten jederzeit über das Vorliegen einer Anordnung und die Dringlichkeit ihrer Umsetzung benachrichtigt werden kann, er eine Anordnung entgegennehmen und Rückfragen zu einzelnen noch nicht abgeschlossenen Überwachungsmaßnahmen entgegennehmen kann. Für Funktionsprüfungen der Aufzeichnungs- und Auswertungseinrichtungen des Bundesnachrichtendienstes gilt § 23 Absatz 1 Satz 1 Nummer 3 entsprechend; für derartige Funktionsprüfungen ist abweichend von § 23 Absatz 1 Satz 8 bis 13 für Maßnahmen nach den §§ 5 oder 8 des Artikel 10-Gesetzes eine Anordnung nach den §§ 5 oder 8 des Artikel 10-Gesetzes und für Maßnahmen nach den §§ 6, 12 oder 14 des BND-Gesetzes eine Anordnung nach § 6 Absatz 1 Satz 2 des BND-Gesetzes erforderlich.

§ 28 Verfahren

(1) Sofern der Verpflichtete für die technische Umsetzung von Anordnungen nach § 5 oder § 8 des Artikel 10-Gesetzes oder Anordnungen für Maßnahmen nach den §§ 6, 12 oder 14 des BND-Gesetzes technische Einrichtungen oder Funktionen verwendet, die durch Eingaben in Steuerungssysteme bedient werden, die von diesen Einrichtungen abgesetzt sind, gelten die §§ 16 und 17 entsprechend.

(2) (weggefallen)

(3) Für den Nachweis der Übereinstimmung der getroffenen Vorkehrungen mit den Bestimmungen dieser Verordnung und der Technischen Richtlinie gilt § 19 entsprechend mit folgenden Maßgaben:

1. An die Stelle der in § 19 Absatz 4 genannten Stellen tritt der Bundesnachrichtendienst.

2. An die Stelle der in § 19 Absatz 5 geforderten Prüfungen tritt eine Prüfung entsprechend § 27 Absatz 2 und 6 bis 8.

(4) Für nachträgliche Änderungen an der Telekommunikationsanlage des Verpflichteten oder an den Überwachungseinrichtungen gilt § 20 entsprechend.

§ 29 Bereitstellung von Übertragungswegen zum Bundesnachrichtendienst

Für die Bereitstellung der Übertragungswege, die zur Übermittlung der gemäß § 27 Absatz 3 Nummer 1 aufbereiteten Kopie an den Bundesnachrichtendienst erforderlich sind, gilt § 24 Absatz 1 Satz 1 und Absatz 2 entsprechend.

Teil 4 Vorkehrungen für die Erteilung von Auskünften über Verkehrsdaten

§ 30 Kreis der Verpflichteten

Die Vorschriften dieses Teils gelten für

1. die Betreiber von Telekommunikationsanlagen, mit denen öffentlich zugängliche Telekommunikationsdienste erbracht werden, sowie

2. die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten

in dem Umfang, in dem diese ihre Dienste für Endnutzer erbringen. *2*§ 110 Absatz 1 Satz 2 des Telekommunikationsgesetzes gilt entsprechend für die nach Satz 1 Verpflichteten, die nur Teile von Telekommunikationsanlagen nach Satz 1 Nummer 1 betreiben oder die öffentlich zugängliche Telekommunikationsdienste erbringen, ohne hierfür Telekommunikationsanlagen zu betreiben.

§ 31 Grundsätze

(1) Die nach § 30 Verpflichteten haben Auskunftsverlangen in einem digitalen Format zu beantworten. Die Anforderungen nach § 14 Absatz 1 und 3 gelten entsprechend.

(2) Die nach § 30 Verpflichteten haben sicherzustellen, dass sie Anordnungen zur Auskunftserteilung jederzeit elektronisch entgegennehmen sowie die zugehörigen Auskünfte auf gleichem Weg erteilen können; dabei haben diejenigen Verpflichteten, die zur Bereithaltung der Schnittstelle nach § 113 Absatz 5 des Telekommunikationsgesetzes verpflichtet sind, diese Schnittstelle auch für die Entgegennahme der Anordnungen zur Auskunftserteilung und für die Übermittlung der zugehörigen Auskünfte zu verwenden und Verpflichtete, die nicht zur Bereithaltung dieser Schnittstelle verpflichtet sind, ein E-Mail-basiertes Übermittlungsverfahren nach Vorgaben der Bundesnetzagentur zu verwenden. Die nach § 30 Verpflichteten haben technisch sicherzustellen, dass sowohl die Anordnung als auch die Auskünfte bei der Übermittlung gegen Veränderungen und unbefugte Kenntnisnahme durch Dritte geschützt sind. Die dafür zu beachtenden technischen Einzelheiten einschließlich der zugehörigen Formate und der zu verwendenden Verschlüsselungsverfahren für die Übermittlung der Anordnung und der Auskünfte legt die Bundesnetzagentur in der Technischen Richtlinie nach § 110 Absatz 3 des Telekommunikationsgesetzes fest. Eine Übermittlung der Anordnung oder der Auskünfte per Telefax ist unzulässig. Für die Benachrichtigung über das Vorliegen einer Anordnung und die Dringlichkeit ihrer Umsetzung, für die Entgegennahme der Anordnung, für den sicheren Umgang mit der Anordnung und deren Umsetzung, für den Schutz der für die Erteilung von Auskünften erforderlichen Funktionen und der dafür vorzuhaltenden technischen Einrichtungen sowie für Rückfragen zu erteilten Auskünften gilt im Übrigen § 12 Absatz 1 Satz 2 und 5, Absatz 2 sowie Absatz 3 entsprechend. Für Rückfragen zu erteilten Auskünften gilt dies mit der Maßgabe, dass der Verpflichtete Rückfragen nur innerhalb seiner üblichen Geschäftszeiten durch sachkundiges Personal zu beantworten braucht.

(3) Die nach § 30 Verpflichteten haben die technischen und organisatorischen Vorkehrungen so zu treffen, dass sie Auskunftsverlangen zu ihnen vorliegenden Verkehrsdaten unverzüglich beantworten können (§ 100b Absatz 3 Satz 1 der Strafprozessordnung); dies gilt auch, wenn für die Auskünfte über gespeicherte Verkehrsdaten zu Verbindungen, die zu einer bestimmten Zieladresse oder von einer bekannten Rufnummer zu unbekannten Zieladressen hergestellt wurden, die Suche in allen Datensätzen der abgehenden oder ankommenden Verbindungen eines Betreibers erforderlich ist (Zielwahlsuche). Für Fälle der Zielwahlsuche gilt abweichend von Absatz 2 Satz 5 auch § 12 Absatz 1 Satz 1 und 3 entsprechend. In der Technischen Richtlinie nach § 110 Absatz 3 des Telekommunikationsgesetzes können in Abhängigkeit von der jeweiligen Netzstruktur und der in dem Netz eingesetzten Technologie angemessene Zeitspannen festgelegt werden, die zwischen der Erhebung der Verkehrsdaten in den Netzelementen und deren Verfügbarkeit für den Abruf höchstens vergehen dürfen.

(4) Die nach § 30 Verpflichteten haben sicherzustellen, dass die Verfügbarkeit ihrer für die Auskunftserteilung erforderlichen technischen Einrichtungen der Verfügbarkeit ihrer Telekommunikationsanlagen entspricht.

(5) Betreiber nach § 30 Satz 1 Nummer 1, mit deren Telekommunikationsanlagen Telekommunikationsdienste für nicht mehr als 100 000 Endnutzer erbracht werden und Anbieter nach § 30 Satz 1 Nummer 2, die ihre Dienste für nicht mehr als 100 000 Endnutzer erbringen, brauchen die Vorkehrungen nach den Absätzen 3 und 4 nicht zu treffen; sie dürfen der Verpflichtung nach Absatz 2 Satz 1 in der Weise nachkommen, dass sie erst nach Benachrichtigung durch die berechtigte Stelle über das Vorliegen einer Anordnung innerhalb ihrer üblichen Geschäftszeiten unverzüglich die Anordnung entgegennehmen und die zugehörigen Auskünfte erteilen. Verpflichtungen nach § 101a Absatz 1 der Strafprozessordnung oder nach den anderen in § 2 Nummer 1 Buchstabe b genannten Vorschriften zur Erteilung von Auskünften über Verkehrsdaten bleiben unberührt.

(6) Für das Treffen der Vorkehrungen nach diesem Teil, die Umsetzung einer Anordnung zur Erteilung von Auskünften über Verkehrsdaten sowie für die Wahrnehmung dieser Aufgaben durch einen Erfüllungsgehilfen gilt § 5 Absatz 3 entsprechend.

(7) Das Übermittlungsverfahren nach Absatz 2 und die dafür vorgehaltenen technischen Einrichtungen dürfen auch genutzt werden für die Übermittlung von:

1. Anordnungen zur Überwachung der Telekommunikation,
2. Auskunftsverlangen zu Bestandsdaten nach § 113 des Telekommunikationsgesetzes,
3. Auskunftsverlangen zu Standortangaben sowie
4. Antworten zu den Auskunftsverlangen nach den Nummern 2 und 3.

§ 32 Auskünfte über zurückliegende Verkehrsdaten, zukünftige Verkehrsdaten, Verkehrsdaten in Echtzeit

(1) Die nach § 30 Verpflichteten haben Auskünfte auf Grundlage der nach den Vorschriften des Telekommunikationsgesetzes gespeicherten und zum Zeitpunkt der Auskunftserteilung vorhandenen Daten zu erteilen. Dabei haben sie stets alle dem Auskunftsverlangen zuzuordnenden Datensätze bereitzustellen, die ihnen zum Zeitpunkt der Auskunftserteilung vorliegen. Datensätze, die erst nach einer technisch bedingten Wartezeit zur Verfügung stehen und einem bereits beauskunfteten Auskunftsverlangen zuzuordnen sind, sind unverzüglich nachträglich zu übermitteln. Die berechtigte Stelle kann bereits bei der erstmaligen Übermittlung des Auskunftsverlangens Anforderungen zur nachträglichen Übermittlung von Datensätzen nach Satz 3 festlegen. Macht sie von dieser Möglichkeit Gebrauch, sind

diese Anforderungen maßgeblich für die nachträgliche Übermittlung nach Satz 3. Die berechtigte Stelle kann im Einzelfall auch auf die nachträgliche Übermittlung verzichten.

(2) In Fällen von Anordnungen zur Erteilung von Auskünften über Verkehrsdaten, die erst nach dem Zeitpunkt der Ausstellung der Anordnung anfallen (zukünftige Verkehrsdaten), haben die nach § 30 Verpflichteten der jeweiligen berechtigten Stelle zu jeder sich auf diese Anordnung stützenden Anforderung Auskünfte über die der Anordnung zuzuordnenden Datensätze zu erteilen, die ihnen zum Zeitpunkt der Auskunftserteilung vorliegen; dabei können sich in jeder aktuellen Auskunftserteilung auch Datensätze befinden, die zu vorhergehenden Anforderungen bereits mitgeteilt wurden. Die Häufigkeit und der Zeitabstand der jeweiligen Anforderungen liegt im ausschließlichen Ermessen der berechtigten Stelle. Im Rahmen von Anordnungen zur Erteilung von Auskünften über zukünftige Verkehrsdaten können auch Auskünfte über Verkehrsdaten verlangt werden, die nach den Vorschriften des Telekommunikationsgesetzes nicht gespeichert, aber im Rahmen des Telekommunikationsvorganges erhoben werden; besondere Vorkehrungen zur Erteilung von derartigen Auskünften müssen jedoch nicht getroffen werden.

(3) Für die Umsetzung von Auskunftsverlangen über Verkehrsdaten in Echtzeit brauchen nur diejenigen Verpflichteten nach § 30 Vorkehrungen zu treffen, die auch nach § 3 verpflichtet sind, technische Vorkehrungen für die Umsetzung von Überwachungsmaßnahmen vorzuhalten. Für die Umsetzung derartiger Auskunftsverlangen gilt abweichend von § 31 Absatz 2 Satz 5 auch § 12 Absatz 1 Satz 1 und 3 entsprechend. Die nach Satz 1 Verpflichteten können zur Umsetzung derartiger Auskunftsverlangen ihre technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen oder Einrichtungen, die in Bezug auf die bereitzustellenden Daten nach § 7 gleichwertig sind, mit der Maßgabe nutzen, dass

1. die an die auskunftsberechtigte Stelle übermittelten Daten keine Nachrichteninhalte enthalten,

2. Standortdaten auch für lediglich empfangsbereite Endgeräte erhoben und an die auskunftsberechtigte Stelle übermittelt werden und

3. die Übermittlung von Standortdaten nach Nummer 2 derart eingeschränkt werden kann, dass sie für die Strafverfolgungsbehörden nur nach Maßgabe des § 100g Absatz 1 der Strafprozessordnung oder für eine andere auskunftsberechtigte Stelle nur nach Maßgabe der für diese Stelle geltenden gesetzlichen Vorschriften erfolgt.

(4) § 6 Absatz 4 gilt entsprechend; in Fällen von zeitweiligen Übermittlungshindernissen, Störungen und Unterbrechungen gelten die §§ 10 und 13 entsprechend.

§ 33 Verschwiegenheit

Für die im Zusammenhang mit Auskunftsverlangen und den dazu erteilten Auskünften zu wahrende Verschwiegenheit gilt § 15 entsprechend.

§ 34 Nachweis, probeweise Anwendungen

(1) Für den Nachweis der Übereinstimmung der getroffenen Vorkehrungen mit den Bestimmungen dieser Verordnung und der Technischen Richtlinie nach § 110 Absatz 3 des Telekommunikationsgesetzes gilt § 19 entsprechend. Außerdem sind in den Unterlagen nach § 19 Absatz 2 auch die gespeicherten Datenarten, die jeweilige Speicherungsdauer und der voraussichtliche Zeitverzug zwischen Erhebung und Verfügbarkeit für deren Abruf zu nennen. Bei nachträglichen Änderungen an den für die Auskunftserteilung vorgehaltenen technischen Einrichtungen gilt § 20 entsprechend.

(2) Für probeweise Anwendungen der technischen Einrichtungen der Verpflichteten nach den §§ 30, 31 und 32 gilt § 23 entsprechend.

§ 35 Protokollierung

Der Verpflichtete hat sicherzustellen, dass die Zugriffe auf seine für die Erteilung von Auskünften vorgehaltenen technischen Einrichtungen automatisch lückenlos protokolliert werden. Dies gilt unabhängig davon, ob die Zugriffe darauf abzielen, Verkehrsdaten zugänglich zu machen, die nach den Vorschriften des Telekommunikationsgesetzes gespeichert wurden, oder Verkehrsdatenübermittlungen in Echtzeit einzurichten. Zu protokollieren sind:

1. die Referenznummer des Auskunftsverlangens, der probeweisen Anwendung nach § 34 Absatz 2 oder einer sonstigen Nutzung der technischen Einrichtungen,
2. die tatsächlich eingegebene Kennung, auf Grund derer die Verkehrsdatensätze ermittelt werden,
3. die weiteren für die Suche verwendeten Daten einschließlich der Zeitpunkte (Datum und Uhrzeit auf der Grundlage der amtlichen Zeit), zwischen denen die Verkehrsdatensätze in Bezug auf die Kennung nach Nummer 2 erfasst werden,
4. die Angabe der Rechtsvorschrift (§ 96 oder § 113b des Telekommunikationsgesetzes), auf deren Grundlage die beauskunfteten Verkehrsdaten gespeichert wurden,
5. die Adressierungsangabe des Anschlusses, an den die ermittelten Verkehrsdatensätze übermittelt werden,
6. ein Merkmal zur Erkennbarkeit der Personen, die die Daten nach den Nummern 1 bis 5 auf Seiten des Verpflichteten eingeben,

7. Datum und Uhrzeit der Eingabe.

Die ermittelten Verkehrsdaten dürfen nicht protokolliert werden. Satz 1 gilt nicht für betrieblich erforderliche Zugriffe auf Daten, die nach § 96 des Telekommunikationsgesetzes gespeichert werden. Die Angaben nach Satz 3 Nummer 6 dürfen ausschließlich bei auf tatsächlichen Anhaltspunkten beruhenden Untersuchungen zur Aufklärung von Missbrauchs- oder Fehlerfällen verwendet werden. Im Übrigen gelten für die Protokollierung sowie für die Prüfung und Löschung der dafür erzeugten Protokolldaten § 16 Absatz 2 und § 17 entsprechend mit der Maßgabe, dass abweichend von § 17 Absatz 1 Satz 3 fünf vom Hundert der gestellten Auskunftsverlangen einer Prüfung zu unterziehen sind.

Teil 5 Ergänzende technische Festlegungen, Übergangsvorschriften, Schlussbestimmungen

§ 36 Technische Richtlinie

Die technischen Einzelheiten zu § 2 Nummer 8 und 17 Buchstabe c, § 4 Absatz 1 und 2, § 5 Absatz 1, 2, 4 Satz 1, Absatz 5 und 6, § 6 Absatz 3, § 7 Absatz 1, 2 und 4, § 8 Absatz 2, § 9 Absatz 1, § 10 Satz 1 und 3, § 12 Absatz 2 Satz 1 und 3, § 14 Absatz 1 und 2 Satz 1, 2, 4 und 5 sowie Absatz 3 Satz 2, § 22 Absatz 1 Satz 5, § 23 Absatz 1 Satz 9 und 12, die erforderlichen technischen Eigenschaften der Aufzeichnungsanschlüsse nach § 24 Absatz 1 Satz 2 sowie die Einzelheiten zur Übermittlung von Auskunftsverlangen und zugehörigen Auskünften nach den §§ 31, 32 und 34 und deren technischen Formate werden von der Bundesnetzagentur unter Beteiligung der Verbände der Verpflichteten, der berechtigten Stellen sowie der Hersteller der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen in einer Technischen Richtlinie festgelegt. Sofern erforderlich, können in der Technischen Richtlinie auch Einzelheiten nach § 27 Absatz 7 Satz 2 und zu § 110 Absatz 1 Satz 1 Nummer 1a des Telekommunikationsgesetzes, soweit sie für das Zusammenwirken von Telekommunikationsanlagen, die von verschiedenen Verpflichteten betrieben werden, notwendig sind, unter Beteiligung der betroffenen Interessenvertreter festgelegt werden. Die Technische Richtlinie wird im gleichen Verfahren an den jeweiligen Stand der Technik angepasst. In der Technischen Richtlinie ist zudem festzulegen, bis zu welchem Zeitpunkt bisherige technische Vorschriften noch angewendet werden dürfen. Die Bundesnetzagentur informiert auf ihrer Internetseite über die anwendbaren Ausgabestände der internationalen technischen Standards, auf die in der Technischen Richtlinie Bezug genommen wird. In der Technischen Richtlinie sind auch die Arten der Kennungen festzulegen, für die bei bestimmten Arten von Telekommunikationsanlagen neben den dort verwendeten Ziel- und Ursprungsadressen auf Grund der die Überwachung der Telekommunikation regelnden Gesetze zusätzliche Vorkehrungen für die technische Umsetzung von Anordnungen zu treffen sind. In Fällen, in denen neue technische Entwicklungen nicht in der Technischen Richtlinie berücksichtigt sind, hat der Verpflichtete die Gestaltung seiner Überwachungseinrichtungen mit der Bundesnetzagentur abzustimmen.

§ 37 Übergangsvorschrift

Für Überwachungseinrichtungen, für die bereits eine Genehmigung nach § 19 der Telekommunikations-Überwachungsverordnung vom 22. Januar 2002 (BGBl. | S. 458), zuletzt geändert durch Artikel 3 Absatz 18 des Gesetzes vom 7. Juli 2005 (BGBl. | S. 1970), oder das Einvernehmen nach § 16 der Fernmeldeverkehr-Überwachungs-Verordnung vom 18. Mai 1995 (BGBl. | S. 722), geändert durch Artikel 4 des Gesetzes vom 26. Juni 2001 (BGBl. | S. 1254), erteilt wurde, ist kein Nachweis nach § 19 erforderlich, sofern die Auflagen aus der Genehmigung erfüllt werden; § 110 Absatz 5 des Telekommunikationsgesetzes bleibt unberührt.

Schlussformel

Der Bundesrat hat zugestimmt.

Anlage (weggefallen)

Anhang 10

Urteile des BVerfG und des EuGH zur Vorratsdatenspeicherung

Urteil des Ersten Senats
des Bundesverfassungsgerichts vom 2. März 2010

Leitsätze:

1. Eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter, wie sie die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 (ABl L 105 vom 13. April 2006, S. 54; im Folgenden: Richtlinie 2006/24/EG) vorsieht, ist mit Art. 10 GG nicht schlechthin unvereinbar; auf einen etwaigen Vorrang dieser Richtlinie kommt es daher nicht an.

2. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die gesetzliche Ausgestaltung einer solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbundenen Grundrechtseingriffs angemessen Rechnung trägt. Erforderlich sind hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes.

3. Die Gewährleistung der Datensicherheit sowie die normenklare Begrenzung der Zwecke der möglichen Datenverwendung obliegen als untrennbare Bestandteile der Anordnung der Speicherungsverpflichtung dem Bundesgesetzgeber gemäß Art. 73 Abs. 1 Nr. 7 GG. Demgegenüber richtet sich die Zuständigkeit für die Schaffung der Abrufregelungen selbst sowie für die Ausgestaltung der Transparenz- und Rechtsschutzbestimmungen nach den jeweiligen Sachkompetenzen.

4. Hinsichtlich der Datensicherheit bedarf es Regelungen, die einen besonders hohen Sicherheitsstandard normenklar und verbindlich vorgeben. Es ist jedenfalls dem Grunde nach gesetzlich sicherzustellen, dass sich dieser an dem Entwicklungsstand der Fachdiskussion orientiert, neue Erkenntnisse und Einsichten fortlaufend aufnimmt und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten steht.

5. Der Abruf und die unmittelbare Nutzung der Daten sind nur verhältnismäßig, wenn sie überragend wichtigen Aufgaben des Rechtsgüterschutzes dienen. Im Bereich der Strafverfolgung setzt dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Für die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste dürfen sie nur bei Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen werden. 1/93

6. Eine nur mittelbare Nutzung der Daten zur Erteilung von Auskünften durch die Telekommunikationsdiensteanbieter über die Inhaber von Internetprotokolladressen ist auch

unabhängig von begrenzenden Straftaten- oder Rechtsgüterkatalogen für die Strafverfolgung, Gefahrenabwehr und die Wahrnehmung nachrichtendienstlicher Aufgaben zulässig. Für die Verfolgung von Ordnungswidrigkeiten können solche Auskünfte nur in gesetzlich ausdrücklich benannten Fällen von besonderem Gewicht erlaubt werden.

Urteil des Europäischen Gerichtshofs vom 8. April 2014:

Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG ist ungültig.

Urteil des Europäischen Gerichtshofs vom 21. Dezember 2016:

1. Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.

2. Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.

3. Die zweite Vorlagefrage des Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) ist unzulässig.

Die vollständigen Urteile sind auf *https://www.bundesverfassungsgericht.de* bzw. *http://curia.europa.eu* zu finden.

Anhang 11

Anschriften der Datenschutzbeauftragten des Bundes und der Länder

Bund	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	Andrea Voßhoff Postfach 14 68 53004 Bonn Husarenstr. 30 53117 Bonn	Tel.: 0228/997799-0 Fax: 0228/997799-5550 E-Mail: poststelle@bfdi.bund.de Internet: www.bfdi.bund.de
Baden-Württemberg	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg	Dr. Stefan Brink Postfach 10 29 32 70025 Stuttgart Königstr. 10a 70173 Stuttgart	Tel.: 0711/615541-0 Fax: 0711/615541-15 E-Mail: poststelle@lfdi.bwl.de Internet: www.baden-wuerttemberg.datenschutz.de
Bayern	Der Bayerische Landesbeauftragte für den Datenschutz	Prof. Dr. Thomas Petri Postfach 22 12 19 80502 München Wagmüllerstr. 18 80538 München	Tel.: 089/212672-0 Fax: 089/212672-50 E-Mail: poststelle@datenschutz-bayern.de Internet: www.datenschutz-bayern.de
Berlin	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Maja Smoltczyk Friedrichstr. 219 10969 Berlin	Tel.: 030/13889-0 Fax: 030/2155050 E-Mail: mailbox@datenschutz-berlin.de Internet: www.datenschutz-berlin.de
Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht	Dagmar Hartge Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 033203/356-0 Fax: 033203/356-49 E-Mail: poststelle@lda.brandenburg.de Internet: www.lda.brandenburg.de
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen	Dr. Imke Sommer Arndtstr. 1 27570 Bremerhaven	Tel.: 0421/361-2010 Fax: 0421/496-18495 E-Mail: office@datenschutz.bremen.de Internet: www.datenschutz.bremen.de
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit	Prof. Dr. Johannes Caspar Kurt-Schumacher-Allee 4 20097 Hamburg	Tel.: 040/42854-4040 E-Fax: 040/ 4279-11811 E-Mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg.datenschutz.de

Hessen	Der Hessische Datenschutz-beauftragte	Prof. Dr. Michael Ronellenfitsch Postfach 31 63 65021 Wiesbaden Gustav-Stresemann-Ring 1 65189 Wiesbaden	Tel.: 0611/1408-0 Fax: 0611/1408-900 E-Mail: poststelle@datenschutz.hessen.de Internet: www.datenschutz.hessen.de
Mecklenburg-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern	Heinz Müller Lennéstr. 1 Schloss Schwerin 19053 Schwerin Werderstr. 74a 19055 Schwerin	Tel.: 0385/59494-0 Fax: 0385/59494-58 E-Mail: info@datenschutz-mv.de Internet: www.datenschutz-mv.de
Niedersachsen	Die Landesbeauf-tragte für den Datenschutz Niedersachsen	Barbara Thiel Prinzenstr. 5 30159 Hannover	Tel.: 0511/120-4500 Fax: 0511/120-4599 E-Mail: poststelle@lfd.niedersachen.de Internet: www.lfd.niedersachsen.de
Nordrhein-Westfalen	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen	Helga Block Postfach 20 04 44 40102 Düsseldorf Kavalleriestr. 2-4 40213 Düsseldorf	Tel.: 0211/38424-0 Fax: 0211/38424-10 E-Mail: poststelle@ldi.nrw.de Internet: www.ldi.nrw.de
Rheinland-Pfalz	Der Landesbeauf-tragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz	Prof. Dr. Dieter Kugelmann Postfach 30 40 55020 Mainz Hintere Bleiche 34 55116 Mainz	Tel.: 06131/208-2449 Fax: 06131/208-2497 E-Mail: poststelle@datenschutz.rlp.de Internet: http://www.datenschutz.rlp.de
Saarland	Unabhängiges Datenschutzzentrum Saarland	Monika Grethel Postfach 10 26 31 66026 Saarbrücken Fritz-Dobisch-Str. 12 66111 Saarbrücken	Tel.: 0681/94781-0 Fax: 0681/94781-29 E-Mail: poststelle@datenschutz.saarland.de Internet: www.datenschutz.saarland.de
Sachsen	Der Sächsische Datenschutz-beauftragte	Andreas Schurig Devrientstr. 1 01067 Dresden	Tel.: 0351/493-5401 Fax: 0351/493-5490 E-Mail: saechsdsb@slt.sachsen.de Internet: www.saechsdsb.de
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt	Dr. Harald von Bose Postfach 19 47 39009 Magdeburg Leiterstr. 9 39104 Magdeburg	Tel.: 0391/81803-0 Fax: 0391/81803-33 E-Mail: poststelle@lfd.sachen-anhalt.de Internet: www.datenschutz.sachsen-anhalt.de

Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Marit Hansen Postfach 71 16 24171 Kiel Holstenstr. 98 24103 Kiel	Tel.: 0431/988-1200 Fax: 0431/988-1223 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit	Dr. Lutz Hasse Postfach 90 04 55 99107 Erfurt Häßlerstr. 8 99096 Erfurt	Tel.: 0361/ 57311-2900 Fax: 0361/ 57311-2904 E-Mail: poststelle@datenschutz.thueringen.de Internet: www.tlfdi.de

Anhang 12

Anschriften der Aufsichtsbehörden für den nicht-öffentlichen Bereich

Baden-Württemberg	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg Königstr. 10a 70173 Stuttgart Tel.: 0711/615541-0 Fax: 0711/615541-15 E-Mail: poststelle@lfdi.bwl.de Internet: www.baden-wuerttemberg.datenschutz.de
Bayern	Bayerisches Landesamt für Datenschutzaufsicht Promenade 27 (Schloss) 91522 Ansbach Tel.: 0981/53-1300 Fax: 0981/53-98-1300 E-Mail: poststelle@lda.bayern.de Internet: www.lda.bayern.de
Berlin	Berliner Beauftragte für Datenschutz und Informationsfreiheit Friedrichstr. 219 10969 Berlin Tel.: 030/13889-0 Fax: 030/2155050 E-Mail: mailbox@datenschutz-berlin.de Internet: www.datenschutz-berlin.de
Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Stahnsdorfer Damm 77 14532 Kleinmachnow Tel.: 033203/356-0 Fax: 033203/356-49 E-Mail: poststelle@lda.brandenburg.de Internet: www.lda.brandenburg.de
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Arndtstr. 1 27570 Bremerhaven Tel.: 0421/361-2010 Fax: 0421/496-18495 E-Mail: office@datenschutz.bremen.de Internet: www.datenschutz.bremen.de
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Kurt-Schumacher-Allee 4 20097 Hamburg Tel.: 040/42854-4040 E-Fax: 040/ 4279–11811 E-Mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg.datenschutz.de

Hessen	Der Hessische Datenschutzbeauftragte Gustav-Stresemann-Ring 1 65189 Wiesbaden Tel.: 0611/1408-0 Fax: 0611/1408-900 E-Mail: poststelle@datenschutz.hessen.de Internet: www.datenschutz.hessen.de
Mecklenburg-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern Werderstr. 74a 19055 Schwerin Tel.: 0385/59494-0 Fax: 0385/59494-58 E-Mail: info@datendschutz-mv.de Internet: www.datenschutz-mv.de
Niedersachsen	Die Landesbeauftragte für den Datenschutz Niedersachsen Prinzenstr. 5 30159 Hannover Tel.: 0511/120-4500 Fax: 0511/120-4599 E-Mail: postelle@lfd.niedersachsen.de Internet: www.lfd.niedersachsen.de
Nordrhein-Westfalen	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Kavalleriestr. 2-4 40213 Düsseldorf Tel.: 0211/38424-0 Fax: 0211/38424-10 E-Mail: poststelle@ldi.nrw.de Internet: www.ldi.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz Hintere Bleiche 34 55116 Mainz Tel.: 06131/208-2449 Fax: 06131/208-2497 E-Mail: poststelle@datenschutz.rlp.de Internet: www.datenschutz.rlp.de
Saarland	Unabhängiges Datenschutzzentrum Saarland Fritz-Dobisch-Str. 12 66111 Saarbrücken Tel.: 0681/94781-0 Fax: 0681/94781-29 E-Mail: poststelle@datenschutz.saarland.de Internet: www.datenschutz.saarland.de

Sachsen	Der Sächsische Datenschutzbeauftragte Devrientstr. 1 01067 Dresden Tel.: 0351/493-5401 Fax: 0351/493-5490 E-Mail: saechsdsb@slt.sachsen.de Internet: www.saechsdsb.de
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt Leiterstr. 9 39104 Magdeburg Tel.: 0391/81803-0 Fax: 0391/81803-33 E-Mail: poststelle@lfd.sachen-anhalt.de Internet: www.datenschutz.sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Holstenstr. 98 24103 Kiel Tel.: 0431/988-1200 Fax: 0431/988-1223 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit Häßlerstr. 8 99096 Erfurt Tel.: 0361/57311-2900 Fax: 0361/57311 -2904 E-Mail: poststelle@datenschutz.thueringen.de Internet: www.tlfdi.de

Stichwortverzeichnis