INFO
05

Datenschutz und Tele-kommunikation

BfDI
Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Impressum

Herausgegeben von:

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Postfach 14 68, 53004 Bonn
Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-5550
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Stand: August 2020

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

Realisation: Appel & Klinger Druck und Medien GmbH

Bildnachweis: Getty Images International

Hinweis zur geschlechtergerechten Formulierung:
Wenn im Text überwiegend die männliche Form verwendet wird,
geschieht dies ausschließlich aus Gründen der Lesbarkeit.
Weiterhin wurden Begrifflichkeiten wie „(Dienste-)Anbieter oder
„Auftragsverarbeiter“ etc. nicht gegendert, um nah
am Gesetzeswortlaut zu bleiben.

Datenschutz und
Telekommunikation

BfDI – Info 5

Inhalt

Vorwort

Telekommunikation ist der Taktgeber unserer digitalen Gesellschaft. Wir alle nutzen ständig das Handy, das Internet und Messenger-Dienste, um zu kommunizieren, zu informieren aber auch um zu arbeiten. Längst sind die Grenzen zwischen Arbeitszeit und Freizeit, zwischen dienstlicher und privater Nutzung unserer Kommunikationsmittel fließend.

In diesem sich ständig wandelnden Umfeld sind verlässliche und klare Datenschutzregeln entscheidend. Die Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 europaweit Anwendung findet, ist hierfür ein Meilenstein. Diese sorgt für EU-weit einheitliche Regeln, die auf viele Dienste anwendbar sind. Leider hält der Telekommunikationsbereich hier noch nicht ganz mit. Insbesondere die europäische E-Privacy-Verordnung, die eigentlich gemeinsam mit der DSGVO in Kraft treten sollte, lässt nach wie vor auf sich warten.

Viele Bürgerinnen und Bürger sind zunehmend sensibel für Datenschutzbelange. Sie nehmen die Verarbeitung ihrer persönlichen Daten nicht mehr einfach hin, sondern machen ihre Rechte gegenüber Unternehmen und Behörden selbstbewusst geltend. Dies zeigen auch die Anfragen und Beschwerden, die an meine Behörde gerichtet werden. Die Zahlen steigen kontinuierlich an. Der Bereich der Telekommunikation steht dabei im besonderen Fokus.

Datenschutz hat ein klares Ziel: Die persönlichen Daten und die Privatsphäre zu schützen! Ich freue mich, wenn sich Bürgerinnen und Bürger für dieses Thema interessieren und sich informieren. Diese Broschüre soll dabei unterstützen. Sie gibt einen Überblick über die wichtigsten Normen im Telekommunikationsbereich und erläutert diese.

Bonn, im August 2020

Prof. Ulrich Kelber
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Abkürzungsverzeichnis

AAV	Automatisiertes Auskunftsverfahren
Abs.	Absatz
AES	Advanced Encryption Standard
AO	Abgabenordnung
APC	Arbeitsplatzcomputer
App	Applikationen
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGBl	Bundesgesetzblatt
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
ca.	cirka
CAT-iq	Cordless Advanced Technology – internet and quality
DECT	Digital Enhanced Cordless Telecommunications
d. h.	das heißt
DIN	Deutsches Institut für Normung
DNS	Domain Name System
DSGVO	Datenschutz-Grundverordnung
DSL	Digital Subscribe Line
EC	Electronic Cash (Girocard)

EG	Europäische Gemeinschaft
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EVN	Einzelverbindungsnachweis
ff.	fortfolgende
GG	Grundgesetz
ggf.	gegebenenfalls
ggü.	gegenüber
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HGB	Handelsgesetzbuch
https	Hypertext Transfer Protocol Secure
ID	Identification
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4/6	Internet Protocol Version 4/6
i. S. d.	im Sinne des
ISDN	Integrated Services Digital Network
IT	Informationstechnik
KDAV	Kundendatenauskunftsverordnung
KRITIS	Kritische Infrastruktur
LTE	Long Term Evolution
MMS	Multimedia Messaging Service
NotrufV	Verordnung über Notrufverbindungen
Nr.	Nummer
OTT	Over-the-Top
OWiG	Gesetz über Ordnungswidrigkeiten

OVG	Oberverwaltungsgericht
PC	Personal Computer
PIN	Personal Identification Number
PUK	Personal Unblocking Key
RL	Richtlinie
RLTk-Bund	Richtlinie Telekommunikation Bund
S.	Satz
SIM	Subcriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service (Kurzmitteilung)
sog.	sogenannt
SSID	Service Set Identifier
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TKÜV	Telekommunikationsüberwachungsverordnung
TLS	Transport Layer Security
TMG	Telemediengesetz
TR	Technische Richtlinie
TR AAV	Technische Richtlinie für das automatisierte Auskunftsverfahren
TR Notruf	Technische Richtlinie Notrufverbindungen
TR TKÜV	Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten
u. a.	unter anderem
UC	Unified Communications

UMTS	Universal Mobile Telecommunications System
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
USA	United States of America
UStG	Umsatzsteuergesetz
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb
vgl.	vergleiche
VLAN	Virtual Local Area Network
VO	Verordnung
VoIP	Voice over IP
VoLTE	Voice over Long Term Evolution
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
z. B.	zum Beispiel
z. T.	zum Teil

1 Überblick über die bereichsspezifischen Regelungen zum Datenschutz in der Telekommunikation

1.1 Grundgesetz

Das Fernmeldegeheimnis ist nach Art. 10 Abs. 1 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 (Art. 10 Abs. 2 GG). Was sich hinter dem Begriff *Fernmeldegeheimnis* verbirgt, verdeutlicht § 88 Abs. 1 TKG. Dabei bezeichnet der Begriff *Inhalt* die mittels Telekommunikationsanlagen übermittelten individuellen Nachrichten, während mit den *näheren Umständen* insbesondere die Verkehrsdaten (siehe Kapitel 2.6) eines Kommunikationsvorganges gemeint sind. Art. 10 GG regelt nur den Schutz des Fernmeldegeheimnisses im Verhältnis zwischen Bürger und Staat. Er hat aber keine unmittelbare Wirkung für den privaten Rechtsverkehr, also weder im Verhältnis zwischen Telekommunikationsdiensteanbietern und ihrer Kundinnen sowie Kunden noch zwischen Privatpersonen.

1.2 Datenschutz-Grundverordnung

Die europäische DSGVO schafft einen unionsweiten allgemeinen Rechtsrahmen für die Verarbeitung personenbezogener Daten. Sie regelt zentrale Grundsätze für die Verarbeitung personenbezogener Daten, die bei jeder Verarbeitung zu befolgen sind. Zu diesen Grundsätzen gehören die Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit.

Eine Konkretisierung des Grundsatzes der Rechtmäßigkeit stellt Art. 6 Abs. 1 DSGVO dar, wonach die Verarbeitung personenbezogener Daten nur rechtmäßig ist, wenn mindestens eine der dort genannten Bedingungen erfüllt ist.

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Dies sind:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische oder biometrische Daten
- Gesundheitsdaten
- sexuelle Orientierung

Art. 9 Abs. 2 DSGVO sieht allerdings abschließende Ausnahmen von diesem Verbot vor.

Zudem finden sich in der DSGVO Transparenz- und Informationspflichten der Verantwortlichen sowie die Rechte betroffener Personen – wie bspw. Recht auf Auskunft, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung oder auf Datenübertragbarkeit.

Als allgemeiner Rechtsrahmen gilt die DSGVO auch für Anbieter öffentlich zugänglicher Kommunikationsdienste, allerdings nur soweit als die E-Privacy-Richtlinie (2002/58/EG) keine Regelungen trifft, die dasselbe Ziel verfolgen; diese werden an späterer Stelle beschrieben.

1.3 Telekommunikationsgesetz

Das TKG 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, siehe 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 den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung ihrer Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen erbringen. Seit Inkrafttreten der DSGVO werden einige datenschutzrechtliche Regelungen des TKG von der DSGVO verdrängt (siehe Kapitel 2.2 und 2.5). Dies betrifft insbesondere Regelungen zu Bestandsdaten, auf die überwiegend nur noch die DSGVO anzuwenden ist.

Verschiedene Bestimmungen des TKG ermächtigen die Bundesregierung, weitere Regelungen bzw. technische Einzelheiten durch Rechtsverordnung zu treffen. Folgende Verordnungen sind hierbei besonders relevant:

- *Telekommunikationsüberwachungsverordnung (TKÜV):*
  Diese Verordnung richtet sich an Anbieter von Telekommunikationsdiensten und legt Anforderungen zu Überwachungsmaßnahmen fest. Die technischen Einzelheiten finden sich in der *Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR TKÜV)*. Dort sind auch Regelungen zur Übermittlung von Anordnungen und Auskünften enthalten (siehe 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 (siehe Kapitel 2.15).

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

1.4 Telemediengesetz

Das TMG 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 und die auf Interaktion angelegten Dienste, wie z. B. Online-Banking und Online-Shops. Das TMG setzt in wesentlichen Teilen die europäische E-Commerce-Richtlinie (2000/31/EG) um. Teile des TMG sind seit Inkrafttreten der DSGVO nicht mehr anwendbar. Im Übrigen gilt das TMG gleichermaßen für privatwirtschaftliche und öffentliche Stellen; die einzelnen Regelungen werden in Kapitel 3.12 erläutert.

1.5 Bundesdatenschutzgesetz

Zur Gültigkeit der DSGVO wurde das bisherige BDSG vollständig neu gefasst (siehe Anhang 3). Es enthält im Wesentlichen nur noch Durchführungsbestimmungen, da das allgemeine Datenschutzrecht mit der DSGVO nunmehr europarechtlich geregelt ist. Seither gelten in der EU die gleichen datenschutzrechtlichen Standards. Eigene datenschutzrechtliche Regelungen können die Mitgliedstaaten nur noch in den Bereichen treffen, in denen die DSGVO nicht anwendbar ist, Ausnahmen vorsieht oder sie nationale Abweichungen zulässt. Einen Überblick über die DSGVO und das aktuelle BDSG vermittelt die Broschüre Info 1 „DSVGO – BDSG; Texte und Erläuterungen“.

Die Info 1 finden Sie als Download auf unserer Webseite www.bfdi.bund.de. Dort können Sie auch eine gedruckte Version kostenfrei bestellen.

1.6 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. Ihr Ziel ist, den besonderen Umständen und Herausforderungen bei der elektronischen Kommunikation als Kernelement der fortschreitenden Digitalisierung Rechnung zu tragen. Darüber hinaus dienen sie dazu, europaweit gleiche Wettbewerbsbedingungen zu schaffen. Damit ist E-Privacy auch einer der Eckpunkte des digitalen Binnenmarkts.

Die Vorschriften zu E-Privacy dienen als spezialgesetzliche Regelung der Konkretisierung und Ergänzung der DSGVO. Die aktuelle E-Privacy-Richtlinie (2002/58/EG) wurde seit 2002 hierbei mehrfach geändert. In Deutschland wurde die E-Privacy-Richtlinie durch Vorschriften im TKG und im TMG, aber z. B. auch im nationalen Wettbewerbsrecht umgesetzt. Soweit die Vorschriften des TKG oder des TMG der Umsetzung der E-Privacy-Richtlinie dienen, bleiben sie gemäß Art. 95 DSGVO vom Anwendungsbereich der DSGVO ausgenommen.

Als Ergebnis einer umfangreichen Evaluation der E-Privacy-Richtlinie hat die Europäische Kommission vorgeschlagen, diese zukünftig durch eine in allen Mitgliedstaaten der 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 die DSGVO an Stelle der E-Privacy-Richtlinie als Spezialgesetz konkretisieren und ergänzen.

Während die Europäische Kommission im Januar 2017 und das Europäische Parlament im Oktober 2017 jeweils einen Entwurf für eine E-Privacy-VO vorgelegt haben, dauern die Verhandlungen im Rat der EU derzeit noch an.

1.7 Urheberrechtsgesetz

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. Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe des UrhG.

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 ein Nutzer eine angebotene Datei auf den eigenen PC heruntergeladen hat, wird diese Datei häufig automatisch auf dem Computer dieses Nutzers zum Download für andere Nutzer angeboten. Das Anbieten einer urheberrechtlich geschützten Datei stellt einen Verstoß gegen das UrhG (siehe Anhang 5) dar. Um solche Verstöße aufzuklären, wenden sich die Rechteinhaber vielfach an die Internet-Zugangsprovider, eine Praxis, die zahlreiche Datenschutzfragen aufwirft (siehe Kapitel 3.10).

1.8 Strafprozessordnung

Jeder Anbieter von Telekommunikationsdiensten ist zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ausnahmen von diesem Grundsatz sind nur dann zulässig, wenn sie gesetzlich angeordnet sind. So finden sich in der 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 (siehe Anhang 6). Von den Regelungen der §§ 113b bis 113f TKG zur sog. Vorratsdatenspeicherung abgesehen (siehe Anhang 1) enthält das TKG für Verkehrsdaten – anders als für Bestandsdaten in § 111 TKG – keine gesonderte Pflicht, Verkehrsdaten vorsorglich für Zwecke der Strafverfolgung zu speichern (siehe Kapitel 3.11). Ab Ergehen einer strafprozessualen Anordnung müssen die nach § 3 TKÜV verpflichteten Dienstanbieter jedoch einzelfallbezogen die in § 7 TKÜV genannten Daten bereitstellen können.

Mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I 2017 S. 3202) wurde in § 100a StPO in Ergänzung zur klassischen TKÜ die Quellen-TKÜ als zusätzliche Maßnahme der Echtzeitüberwachung von Telekommunikationsvorgängen eingeführt. Diese dient der Überwachung verschlüsselter Kommunikation, indem die Daten nicht beim Telekommunikationsanbieter, sondern beim Betroffenen erhoben werden, wo sie unverschlüsselt vorliegen. Diese neu eingeführte Regelung führt nach Auffassung des 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 Art. 10 Abs. 1 GG, der lediglich die Bürgerinnen und Bürger vor Eingriffen des Staates schützt, auf das Verhältnis zwischen Privaten untereinander. Dies ist erforderlich, da Telekommunikationsdienstleistungen meist nicht mehr durch staatliche Stellen, sondern durch private Anbieter erbracht werden.

Schutzbereich

Der Schutzbereich des § 88 TKG entspricht dem des Art. 10 Abs. 1 GG. Geschützt sind neben dem Inhalt der Kommunikation – und zwar unabhängig vom konkret genutzten 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 Telekommunikationsverkehr um- oder weiterleiten, das Umleiten, bei virtuellen Anschlüssen die jeweils zugeordneten physikalischen Anschlüsse,

- bei Mobilfunkanschlüssen 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 bei einem Anbieter von Telekommunikationsdiensten theoretisch in die Lage versetzt werden, Kenntnis über geschützte Kommunikationsvorgänge zu erhalten.

Auch die Anbieter von sog. „OTT“-Kommunikationsdiensten (wie z. B. Messenger-Diensten), deren Nutzung in vielen Bereichen klassische Telekommunikationsangebote wie z. B. die SMS nicht nur überholt, sondern fast schon verdrängt hat, sind 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 (siehe Kapitel 2.7), die Störungsbeseitigung (siehe Kapitel 2.10) oder eine spezielle gesetzliche Vorschrift eine Kenntnisnahme erforderlich macht, z. B. bei strafprozessualen Auskunftsersuchen nach § 100g StPO (siehe Kapitel 3.11). Die in diesem Zusammenhang gewonnenen Kenntnisse über Umstände, die unter das Fernmeldegeheimnis fallen, müssen – auch über den Zeitpunkt der Verpflichtung hinaus – geheim gehalten werden.

Verstöße gegen das Fernmeldegeheimnis

Verstöße gegen das Fernmeldegeheimnis können eine Straftat nach § 206 StGB darstellen und mit einer Geldstrafe oder Freiheitsstrafe bis zu fünf Jahren geahndet werden (siehe Anhang 7). Unter Umständen können daneben noch zivilrechtliche Schadensersatz- und Unterlassungsansprüche entstehen.

2.2 Anwendungsbereich

Die Datenschutzbestimmungen im TKG schützen personenbezogene Daten von Teilnehmerinnen und Teilnehmern bzw. Nutzerinnen und Nutzern, die mit dem geschäftsmäßigen Erbringen eines öffentlich zugänglichen Telekommunikationsdienstes von dessen Anbieter verarbeitet werden (§ 91 TKG). Der Schutz personenbezogener Daten bei nicht-öffentlich zugänglichen Telekommunikationsdiensten richtet sich hingegen nach der DSGVO, weil die E-Privacy-Richtlinie (2002/58/EG) diese Verarbeitungen als Voraussetzung für entsprechendes nationales Recht nicht mitumfasst und infolgedessen nunmehr der Anwendungsvorrang der DSGVO das TKG insoweit verdrängt.

Telekommunikationsdiensteanbieter

Diensteanbieter ist nach § 3 Nr. 6 TKG jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Es handelt sich bei einem Telekommunikationsdienst um einen Dienst, der in der Regel gegen Entgelt erbracht wird und ganz oder überwiegend der Signalübertragung dient (§ 3 Nr. 24 TKG). Handelt es sich um Leistungspakete, etwa bei Hotels und Cafés, die Beherbergung/Bewirtung und WLAN gemeinsam anbieten (siehe Kapitel 4.4.2), muss zunächst geprüft werden, ob der Übertragungsdienst – hier das WLAN – aus Nutzer- und Anbietersicht funktional separat von den anderen Leistungen – hier der Beherbergung/Bewirtung – betrachtet werden kann. In den genannten Beispielen ist dies der Fall. Abzustellen ist somit allein auf das WLAN, das überwiegend der Signalübertragung dient und somit einen Telekommunikationsdienst darstellt. Unter Zugrundelegung dieser Maßstäbe sind auch Arbeitgeber, die ihren Beschäftigten die private Nutzung der betrieblichen Telekommunikationsinfrastruktur erlauben, Telekommunikationsdiensteanbieter (siehe Bundestagsdrucksachen 13/3609, S. 53 und 17/4230, S. 43). Auch einzelne sog. „Over-The-Top"-Kommunikationsdienste (OTT-Dienste) wie Messenger-Dienste, die für ihr Angebot keine eigenen Netze, sondern eine unabhängig von ihrem Dienst bestehende Internetverbindung nutzen, können als Telekommunikationsdienst angesehen werden. Mit Urteil vom 13. Juni 2019 (C-193/18) hat der EuGH entschieden, dass ein E-Mail-Dienst kein „elektronischer Kommunikationsdienst" im Sinne der Kommunikations-Rahmen-RL ist. Folglich unterfallen diese Dienste auch nicht der Definition des § 3 Nr. 24 TKG. Eine Änderung tritt ab Dezember 2020 ein, wenn der Kodex für elektronische Kommunikation (RL 2018/1972) ins nationale Recht umgesetzt wird.

Teilnehmer und Nutzer

Da der Anwendungsbereich nach § 91 Abs. 1 S. 1 TKG die Verarbeitung personenbezogener Daten voraussetzt, kommen zunächst einmal lediglich natürliche Personen als von der Datenverarbeitung betroffene Teilnehmer und Nutzer in Frage. Allerdings erweitert § 91 Abs. 1 S. 2 TKG den Anwendungsbereich auch auf juristische Personen und Personengesellschaften, sofern es sich um Daten handelt, die dem Fernmeldegeheimnis (siehe Kapitel 2.1) unterliegen. Deswegen gelten

die §§ 93 ff. TKG, die die Verarbeitung von Verkehrsdaten (siehe Kapitel 2.6) regeln, auch für juristische Personen und Personengesellschaften, während Vorschriften zum Umgang mit Bestandsdaten (siehe Kapitel 2.5) insoweit nur einschlägig sind, wenn Daten natürlicher Personen betroffen sind.

2.3 Informationspflichten

Anstelle der in § 93 Abs. 1 S. 1 und 3 TKG geregelten Informationspflichten für Diensteanbieter treten seit dem 25. Mai 2018 die Informationspflichten nach Art. 13 und 14 DSGVO.

Bereits bei der erstmaligen Erhebung von personenbezogenen Daten (in der Regel beim Vertragsschluss) müssen den Teilnehmern Name und Kontaktdaten des für die Verarbeitung Verantwortlichen mitgeteilt und die Teilnehmer allgemein darüber unterrichtet werden, welche Art von Daten zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeitet werden (vgl. Kapitel 3.6). Auch sind die Empfänger oder Kategorien von Empfängern zu nennen, an die die personenbezogenen Daten übermittelt werden. Ist eine Übermittlung in ein Drittland, also ein Land außerhalb der EU und des Europäischen Wirtschaftsraumes, beabsichtigt, muss dies ebenfalls angegeben werden. Damit Betroffene wissen, wer der korrekte Ansprechpartner im Unternehmen für datenschutzbezogene Anliegen ist, müssen auch die Kontaktdaten des betrieblichen Datenschutzbeauftragten mitgeteilt werden. Ferner muss auf bestehende Betroffenenrechte – etwa das Recht auf Berichtigung oder Löschung – sowie auf das Beschwerderecht bei der zuständigen Datenschutzbehörde hingewiesen werden.

2.4 Elektronische Einwilligung

Die datenschutzrechtlichen Regelungen folgen dem Grundsatz, dass die Verarbeitung personenbezogener Daten immer nur auf Grundlage einer Einwilligung der betroffenen Person oder einer sonstigen gesetzlich geregelten Grundlage erfolgen darf (Art. 8 Abs. 2 S. 1 EU-Grundrechtecharta). Die Wirksamkeit einer Einwilligung unterliegt nach Art. 4 Nr. 11 sowie Art. 7 und 8 DSGVO gewissen Bedingungen (siehe Kapitel 3.1).

Demnach hat der Diensteanbieter Folgendes sicherzustellen:

- Die Einwilligung wird freiwillig für den bestimmten Fall in informierter Weise und unmissverständlich erteilt. Dies setzt voraus, dass der Nutzer oder Teilnehmer hinreichend über die Voraussetzungen und Folgen seiner Einwilligung informiert ist und die Erklärung (bspw. der Text hinter dem Kästchen, das angeklickt werden muss) eindeutig und verständlich ist.
- Der Umstand, dass eine Einwilligungserklärung abgegeben wurde, muss nachweisbar sein.
- 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.

Im Hinblick auf die Form der Einwilligung kann diese schriftlich, elektronisch oder mündlich erfolgen. § 94 TKG wird seit dem 25. Mai 2018 von der DSGVO verdrängt, da diese Vorschrift nicht auf den Vorgaben der E-Privacy-RL beruht.

2.5 Bestandsdaten

Kundendaten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, bezeichnet das TKG als Bestandsdaten (§ 3 Nr. 3 TKG). Die Zulässigkeit der Verarbeitung der Bestandsdaten richtet sich im Wesentlichen nach der DSGVO. Auch wenn § 95 TKG den Umgang der Diensteanbieter mit Bestandsdaten regelt, ist dieser aufgrund des Anwendungsvorrangs der DSGVO weitgehend nicht anwendbar.

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. Bei im Voraus bezahlten Mobilfunkdiensten (Prepaid-Tarifen) ist der Diensteanbieter verpflichtet, die Identität der Kunden zwecks etwaiger späterer Auskunftsersuchen der Sicherheitsbehörden zu überprüfen (§ 111 Abs. 1 S. 3 TKG).

Ist dagegen der Diensteanbieter vorleistungspflichtig, darf er die Identität nur insoweit prüfen, wie dies für seine eigenen betrieblichen Zwecke erforderlich ist. Kann in diesen Fällen die Identitätsprüfung nicht abschließend vor Ort durchgeführt werden, kann der Diensteanbieter Personalausweiskopien anfertigen. Hierbei ist darauf zu achten, dass nicht benötigte Angaben geschwärzt werden. Die Kopien sind vom Diensteanbieter unverzüglich nach abgeschlossener Überprüfung zu vernichten.

Auch die Vorlage der EC-Karte zur Überprüfung, ob die Angaben im Antrag stimmen, ist zulässig. Die Anfertigung einer Kopie durch den Diensteanbieter ist hierzu regelmäßig nicht erforderlich. Sofern ausnahmsweise eine Kopie erforderlich sein sollte, sind die nicht benötigten Daten – wie z. B. Kartennummer und Gültigkeitsdatum – zu schwärzen.

Bei telefonischen Vertragsabschlüssen wird das Telefonat häufig zu Dokumentations- oder Schulungszwecken dokumentiert. Vor der Einwilligung der Kundinnen und Kunden in diese Aufzeichnung muss der Diensteanbieter auf den Zweck des Gesprächsmitschnittes hinweisen (siehe Kapitel 4.7).

Häufig wird bei Vertragsabschluss auch eine Prüfung der Kreditwürdigkeit (Bonitätsprüfung) durchgeführt; dabei werden die Daten an Auskunfteien übermittelt. Dies ist zulässig, wenn ein Postpaid-Vertrag abgeschlossen werden soll, der Diensteanbieter also in Vorleistung tritt und der Kunde erst nach erhaltener Leistung zahlt (siehe Kapitel 3.4). Der Diensteanbieter hat dann ein berechtigtes Interesse an der Anfrage bei einer Auskunftei (Art. 6 Abs. 1 S. 1 Buchst. f DSGVO). Anders verhält es sich bei Prepaid-Angeboten, bei denen der Diensteanbieter nicht in Vorleistung treten muss. Hier findet eine Bonitätsprüfung in der Regel nicht statt und wäre datenschutzrechtlich auch nicht zulässig.

Löschung der Bestandsdaten

Der Diensteanbieter muss die Bestandsdaten löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Gespeichert werden die Bestandsdaten für den Kundensupport, für die Rechtsabteilung, die Buchhaltung sowie für Auskunftsersuchen der Sicherheitsbehörden. Soweit die Speicherung ausschließlich aufgrund gesetzlicher Speicherpflichten erfolgt (§§ 238, 257 HGB, § 147 AO,

§ 14b UStG, § 111 Abs. 5 TKG), hat nach Ablauf der dort normierten Fristen eine Löschung zu erfolgen. Im Übrigen erfolgt die Speicherung solange, wie der Diensteanbieter eine Erforderlichkeit nachweisen kann. In jedem Fall ist durch technische und organisatorische Maßnahmen sicherzustellen, dass nur diejenigen Personen auf die Daten zugreifen können, die einen solchen Zugriff auch benötigen. So benötigen etwa mehrere Jahre nach Vertragsbeendigung die Mitarbeiter des Kundensupports keinen Zugriff mehr auf Bestandsdaten, die ausschließlich zur Erfüllung handels- und steuerrechtlicher Aufbewahrungspflichten durch die Buchhaltung gespeichert werden dürfen.

Werbung

Der Diensteanbieter darf Rufnummern von Verbrauchern nur dann auf der Grundlage von Art. 6 Abs. 1 S. 1 Buchst. f DSGVO für Werbeanrufe verarbeiten, wenn diese vorher ausdrücklich eingewilligt haben (§ 7 Abs. 2 Nr. 2 UWG). Hintergrund dieser Opt-in-Lösung ist, dass Werbeanrufe für Verbraucher besonders lästig sein können. Bewirbt der Diensteanbieter dagegen seine eigenen Angebote durch Textnachrichten, gilt eine Opt-out-Lösung, so dass die Telefonnummer sowie die Adresse, auch die E-Mail-Adresse, auch ohne Einwilligung verarbeitet werden darf, solange der Kunde einer solchen Verwendung nicht widersprochen hat (§ 95 Abs. 2 S. 2 und 3 TKG). Diese Möglichkeit gilt aber nur bei einer bestehenden Kundenbeziehung und nur für Eigenwerbung der Unternehmen. Außerdem muss der Kunde bei der erstmaligen Erhebung, Speicherung der Rufnummer oder (elektronischen) Adresse sowie bei jeder Versendung einer Nachricht darüber informiert werden, dass er jederzeit der Nutzung seiner Daten für Werbezwecke widersprechen kann. Außerhalb bestehender Kundenbeziehungen bedarf die Verarbeitung von E-Mail-Adressen zu Werbezwecken der Einwilligung (§ 7 Abs. 2 Nr. 3 UWG). Andernfalls ist die Verarbeitung für Werbezwecke unzulässig.

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 sowie diverse technische Infor-

mationen 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 EVN (siehe Kapitel 2.9),
- Störungsbeseitigung und Missbrauchserkennung (siehe Kapitel 2.10),
- Vermarktung, bedarfsgerechte Gestaltung von TK-Diensten und Bereitstellung von Diensten mit Zusatznutzen, wenn der Teilnehmer eingewilligt hat und
- Abrechnung der Telekommunikationsanbieter untereinander (siehe Kapitel 2.7).

Mit den *anderen Gesetzen* sind u. a. Regelungen für Sicherheitsbehörden (siehe Kapitel 3.11) 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 in § 113b TKG vorgesehen.

Die aktuelle Vorratsdatenspeicherung wurde im Frühjahr 2015 mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten beschlossen, nachdem die erste gesetzliche Regelung zur Vorratsdatenspeicherung im Jahr 2010 vom BVerfG für verfassungswidrig erklärt wurde. Im Rahmen der Umsetzung der Entscheidung des BVerfG wurden in § 113b TKG 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 EuGH aus Dezember 2016 (EuGH [Große Kammer], Urteil vom 21.12.2016 – C-203/15,

C-698/15) und einer darauf bezugnehmenden Entscheidung des OVG des Landes Nordrhein-Westfalen in einem Verfahren des einstweiligen Rechtsschutzes (OVG Münster, Beschluss vom 22.6.2017 – 13 B 238/17) hat die BNetzA auf Maßnahmen zur Durchsetzung der Speicherverpflichtung vorläufig verzichtet. Deshalb war zur Zeit der Drucklegung dieser Broschüre die Vorratsdatenspeicherung praktisch ausgesetzt.

Die in § 96 Abs. 1 S. 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 (siehe www.bfdi.bund.de).

Die Regelung zur Nutzung der Verkehrsdaten zur Vermarktung von Telekommunikationsdiensten und anderen in § 96 Abs. 3 TKG aufgeführten Zwecken erlaubt den Anbietern, der jeweiligen Person individuell angepasste Vorschläge für einen Tarifwechsel zu unterbreiten. Voraussetzung ist jedoch eine informierte Einwilligung (siehe 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 Frist von ca. drei Monaten ausreichen, da ein Unternehmen für acht Wochen nach Zugang der Rechnung noch Beanstandungen bearbeiten muss (§ 45i Abs. 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 EVN verlangt wird (siehe Kapitel 2.9). Dies ermöglicht es, im Einzelfall einen nachträglichen EVN 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 bei 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 *Flatrate-Gespräche*. Bei einer echten Flatrate steht das Entgelt fest, ohne die Verkehrsdaten hierfür auswerten zu müssen.

Netzbetreiber erheben Entgelte, wenn sie Gespräche von anderen Netzbetreibern entgegennehmen. Um hier eine Abrechnung zwischen den Netzbetreibern 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 ist und mobil telefonieren, SMS versenden, chatten oder im Internet surfen kann. 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. Bei den meisten Tarifen sind die Standortdaten zur Abrechnung nicht erforderlich, können also – spätestens bei der Rechnungserstellung – gelöscht werden.

Das TKG regelt den Umgang mit Standortdaten, die bei der Telekommunikation von den Netzbetreibern erfasst werden. Dies ist insbesondere der Fall, wenn ein Mobilfunknetz feststellt, in welcher Funkzelle sich das Mobiltelefon befindet. Dadurch kann auch ein einfaches klassisches Handy geortet werden. Diese Regelungen würden aber auch für einen Dienst gelten, bei dem der Standort über Satellitenortung festgestellt aber für einen Telekommunikationsdienst verwendet wird. Die deutlich relevantere 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 ggü. dem Ortungsdiensteanbieter erforderlich. Weiterhin ist bei jeder Ortung eine Textmitteilung, d. h. eine SMS, an das geortete Mobiltelefon 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 bzw. gestohlenen 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 *Mitbenutzenden* (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. Auf eine nach Einzelverbindungen aufgeschlüsselte Rechnung haben Kundinnen und Kunden einen gesetzlichen Anspruch (§ 45e Abs. 1 S. 1 TKG).

§ 99 Abs. 1 S. 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 Abs. 1 S. 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 Abs. 1 S. 2 TKG);
- Beginn und Ende der Verbindung oder die Dauer sind notwendige Angaben sowie
- 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 Abs. 1 S. 7 TKG). Hiermit soll verhindert werden, dass die Anbieter von kostenfrei anrufbaren Werbeplattformen quasi automatisch die Rufnummern ihrer Gesprächspartner erfahren, die sie – etwa über die Inverssuche in Telefonverzeichnissen (siehe Kapitel 2.14) – sogar namentlich zuordnen können.

Darüber hinaus gibt es in § 99 Abs. 1 S. 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, über die Verwendung von EVN informiert zu haben. Auch künftige Mitbenutzerinnen und Mitbenutzer sind unverzüglich zu informieren. Das gleiche gilt bei Anschlüssen in Betrieben und Behörden. Hier muss auch schriftlich erklärt werden, dass die Beschäftigten und künftigen Beschäftigten informiert wurden bzw. werden. Darüber hinaus muss erklärt werden, ob die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich sei. Dieser Mitbenutzerschutz gilt auch dann, wenn ein Arbeitgeber seinen im Außendienst tätigen Beschäftigten 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 Abs. 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- und Verkehrsdaten (siehe Kapitel 2.5 bzw. 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 permanent die entsprechenden Datenflüsse. Sie dürfen gemäß § 100 Ab. 1 TKG für diesen Zweck Bestands- und Verkehrsdaten erheben und verwenden. Der 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 (siehe Kapitel 4.4.1).

Soweit die Daten nicht automatisiert erhoben und verwendet werden, gibt es zudem eine Berichtspflicht ggü. dem BfDI und der BNetzA sowie eine Benachrichtigungspflicht ggü. dem Betroffenen, wenn dieser ermittelt werden kann.

Sofern erforderlich, kann sich der Diensteanbieter zur Störungsbeseitigung nach § 100 Abs. 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 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 Abs. 3 TKG die Verwendung von Verkehrsdaten, um bspw. Leistungserschleichungen oder Betrug feststellen zu können. 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 bei 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 Teilnehmern, 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, muss der Teilnehmer ggü. seinem Diensteanbieter schriftlich darlegen, dass auf seinem Anschluss bedrohende oder belästigende Anrufe ankommen. Dieser überprüft lediglich die Schlüssigkeit des Antrages, nicht jedoch, ob die vorgetragene Bedrohungslage oder Belästigung tatsächlich gegeben ist.

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 Teilnehmer 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 dem Teilnehmer mitgeteilt; der Diensteanbieter dokumentiert das gesamte Verfahren.

Information der *„gefangenen“* Anschlussinhaber

Der Inhaber des Anschlusses, von dem die festgestellten Verbindungen ausgegangen sind, wird nach Abschluss des Verfahrens darüber informiert, dass seine Daten unter den voran genannten Voraussetzungen einem Dritten mitgeteilt worden sind. Von einer solchen Benachrichtigung kann abgesehen werden, wenn der Antragsteller schriftlich und schlüssig dargelegt hat, dass ihm wesentliche Nachteile entstehen könnten, sollten die Inhaber der so festgestellten Anschlüsse informiert werden. In diesem Fall hat der Diensteanbieter abzuwägen, ob die vom Antragsteller 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 bspw. 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 voran genannten Voraussetzungen gestellt werden; keinesfalls darf die Fangschaltung zu einer Dauereinrichtung werden.

Keine präventive Fangschaltung

§ 101 TKG kann 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 (siehe Kapitel 3.11) muss in diesen Fällen von den zuständigen Sicherheitsbehörden unter Berufung auf die entsprechenden Rechtsgrundlagen (z. B. § 100g StPO) angeordnet werden.

2.12 Rufnummernunterdrückung

Private Nutzerinnen und Nutzer 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 Abs. 1 TKG regelt, dass Diensteanbieter, die die Anzeige der Rufnummer auf dem Display des Endgerätes anbieten, ihren 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 Abs. 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 Abs. 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 Abs. 4 S. 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 Abs. 4 S. 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 Abs. 4 S. 3 TKG).

Bei Kundinnen und Kunden, die nicht in ein Teilnehmerverzeichnis eingetragen sind, muss nach § 102 Abs. 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 oder 124 124 hat der Diensteanbieter sicherzustellen, dass eine Anzeige der Rufnummer in jedem Fall erfolgt (§ 102 Abs. 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 Mitbenutzer dürfen nur eingetragen werden, soweit diese sich damit einverstanden erklären (§ 104 S. 3 TKG).

Bei einem Eintrag von Daten in öffentliche elektronische Kundenverzeichnisse sollte sich jeder Kunde darüber im Klaren sein, dass sein 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 datenschutz-

rechtlich vorgesehenen Sanktionen oder zivilrechtlichen Ansprüchen geschädigter Betroffener rechnen. So kann der betroffene Kunde bei Zuwiderhandlungen seine Interessen rechtlich durchsetzen. Nach Art. 82 Abs. 1 DSGVO hat er einen Rechtsanspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter, wenn ihm ein materieller oder immaterieller Schaden entstanden ist. Allerdings entfällt diese Schadensersatzpflicht, wenn die verantwortliche Stelle nachweist, in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich zu sein (Art. 82 Abs. 3 DSGVO). Bei der Durchsetzung dieses Rechtsanspruches ist ausschließlich der zivile Rechtsweg gegeben.

2.14 Telefonauskunft

Nach § 105 Abs. 1 TKG darf im Einzelfall Auskunft über die in öffentlichen Kundenverzeichnissen enthaltenen Rufnummern erteilt werden (Telefonauskunft). Die Kunden sind über ihre Wahl- und Gestaltungsmöglichkeiten zu informieren.

Das TKG regelt in § 105 Abs. 2 S. 1 und 2, dass

- die Telefonauskunft über Rufnummern von 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 der Teilnehmer in eine weitergehende Auskunftserteilung eingewilligt hat.

Die sog. *Inverssuche* regelt Abs. 3 der Norm: Namen und/oder Anschrift eines Teilnehmers, von dem nur die Rufnummer bekannt ist, darf die Telefonauskunft nur weitergeben, wenn der in ein Teilnehmerverzeichnis eingetragene Teilnehmer nach einem Hinweis seines Diensteanbieters auf sein Widerspruchsrecht nicht widersprochen hat.

Ein Widerspruch nach Abs. 2 S. 1 oder Abs. 3 oder eine Einwilligung nach Abs. 2 S. 2 sind in den Kundendateien des Diensteanbieters und des Anbieters nach Abs. 1, die den Verzeichnissen zu Grunde liegen,

- gemäß § 105 Abs. 4 S. 1 TKG *unverzüglich* zu vermerken und

→ gemäß S. 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 Abs. 1 vermerkt ist.

Selbstverständlich können die Kunden ihr Einverständnis jederzeit durch eine entsprechende Erklärung ggü. dem Diensteanbieter zurückziehen; ebenso ist ein Widerspruch jederzeit möglich. Bei einem Anbieterwechsel müssen die 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 NotrufV und die gültige TR 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.

Eine Verbesserung der Genauigkeit des ermittelten Standorts durch Standortangaben von Mobilgeräten, z. B. durch Satellitenortung, ist aufgrund europäischer Regelungen, die Ende 2020 in nationales Recht umzusetzen sind, vorgesehen. Bereits heute gibt es technische Möglichkeiten zur genaueren Standortbestimmung bei Smartphones, die bisher bei einigen Rettungsleitstellen erprobt werden. Diese können etwa aufgrund von Art. 6 Abs. 1 Buchst. d DSGVO als zulässig erachtet werden. Die Thematik wird derzeit noch diskutiert.

2.16 Technische Schutzmaßnahmen

Wer öffentliche Telekommunikationsdienste erbringt oder an der Erbringung dieser Dienste mitwirkt, z. B. durch Bereitstellung von Netzen, hat die ihm anvertrauten personenbezogenen Daten zu schützen und das Fernmeldegeheimnis zu wahren. Die für den Schutz erforderlichen technischen und sonstigen Maßnahmen werden durch das TKG und die DSGVO abstrakt umschrieben.

Telekommunikationsdienstleister haben gemäß § 109 TKG erforderliche technische Vorkehrungen und sonstige Maßnahmen zu treffen, um den Schutz des Fernmeldegeheimnisses und der personenbezogenen Daten zu gewährleisten. Im Katalog von Sicherheitsanforderungen nach § 109 Abs. 6 TKG werden einige konkrete Anforderungen aufgeführt. Netzbetreiber und Erbringer von Diensten haben gemäß § 109 Abs. 4 TKG ein Sicherheitskonzept zu erstellen, Netzbetreiber müssen dies auch der BNetzA vorlegen.

Mit der DSGVO wird der Schutz der personenbezogenen Daten noch unterstrichen. So wird durch Art. 5 Abs. 1 Buchst. f DSGVO gefordert, eine angemessene Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen zu gewährleisten. Mit den Art. 24, 25 und 32 DSGVO werden die Vorgaben weiter konkretisiert. So sind für jede Verarbeitung von personenbezogenen Daten das Risiko für die Verarbeitung zu ermitteln und unter Berücksichtigung des Stands der Technik, der Umsetzungskosten sowie der näheren Umstände und Zwecke der Verarbeitung geeignete technische Maßnahmen einzusetzen. § 109 TKG bleibt grundsätzlich gültig; dort wo er nicht anwendbar ist, sind die Regelungen der DSGVO anzuwenden. Konkret ist § 109 Abs. 1 TKG nicht vollumfänglich durch RL 2002/58/EG (e-Privacy) begründet, sodass für Bestandsdaten die DSGVO Anwendung findet.

Die Maßnahmen müssen sowohl zum Zeitpunkt der Festlegung als auch zum Zeitpunkt der stattfindenden Verarbeitung die geforderten Bedingungen erfüllen. Es sind auch Prozesse vorzusehen, welche die Wirksamkeit der Maßnahmen einer regelmäßigen Prüfung unterziehen, um die Angemessenheit der Maßnahme zu prüfen. Dies bedeutet, dass die Unternehmen sich auf neue Gefährdungsszenarien einstellen und die eingesetzten Maßnahmen im Bedarfsfall ersetzen, wenn das notwendige Schutzniveau nicht mehr erreicht wird.

Als technische Maßnahme wird explizit die Verschlüsselung von personenbezogenen Daten genannt, die für die Speicherung von Zugangskennwörtern als auch für die Übermittlung von Kommunikationsinhalten zum Tragen kommt. Bei der Wahl der jeweiligen Verschlüsselungsalgorithmen können sich die Unternehmen an den Veröffentlichungen des BSI orientieren. Das BSI publiziert das Grundschutzkompendium, die technischen RL und weitere Schriften. Die Publikationen des BSI werden stets aktualisiert und erweitert. Sie stellen den anwendbaren Stand der Technik dar, der auf die individuellen Geschäftsprozesse des einzelnen Telekommunikationsunternehmens angepasst werden muss.

Öffentlich zugängliche Telekommunikation wird in Deutschland als kritische Infrastruktur angesehen. Kritische Infrastrukturen sind per Definition Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Insofern sind für diese Infrastrukturen bestimmte Maßnahmen (Zugangssicherung etc.) umzusetzen, die z. T. über den Anforderungshorizont der DSGVO hinausgehen.

2.17 Meldepflicht bei datenschutzrelevanten Datensicherheitsvorfällen und Schadsoftware

Anbieter öffentlich zugänglicher Telekommunikationsdienste müssen nach § 109a TKG und Art. 33 DSGVO Vorfälle melden, bei denen der durch das TKG bzw. die DSGVO bezweckte Schutz der von ihnen verarbeiteten personenbezogenen Daten verletzt wurde. Diese gesetzliche Informationspflicht ist zweigliedrig ausgestaltet.

Meldung an die Aufsichtsbehörden

Eine Meldung muss – unabhängig von den Umständen des zu meldenden Vorfalls – im Fall des 109a TKG immer ggü. der BNetzA und dem BfDI erfolgen. Fälle nach Art. 33 DSGVO sind nur an den BfDI zu melden. Für beide Fallkonstellationen stehen den Telekommunikationsdienstleistern entsprechende Meldeformulare zur Verfügung. Geringfügige Datenschutzverletzungen nach der DSGVO, die voraussichtlich nicht zu einem Risiko für die Betroffenen führen, müssen

nicht gemeldet werden. Die Meldepflicht nach § 109a Abs. 1 S. 1 TKG gilt hingegen unbeschränkt, so dass auch vermeintlich kleinere Vorfälle mit potenziell weniger schweren Auswirkungen den Aufsichtsbehörden mitzuteilen sind. BNetzA und BfDI haben für die Meldungen nach § 109a TKG gemeinsame Leitlinien für die Telekommunikationsdienstleister erstellt. Diese können über die Internetauftritte 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 (§ 109a Abs. 1 S. 2 TKG) bzw. die Datenschutzverletzung für diese voraussichtlich ein hohes Risiko zur Folge hat (Art. 34 DSGVO). Hierdurch sollen Betroffene in die Lage versetzt werden, eigene Schutzvorkehrungen zu treffen, um nachteilige Folgen der Datenschutzverletzung zu 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, wie mögliche nachteilige Auswirkungen des Vorfalls begrenzt werden 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. Soweit diese Vorfälle ggü. den Aufsichtsbehörden meldepflichtig sind, prüfen diese, ob die Entscheidung, auf eine Benachrichtigung zu verzichten, rechtmäßig getroffen wurde und wirken andernfalls auf eine Nachholung der Benachrichtigung hin.

Verzeichnis der Datenschutzverletzungen

Neben der Melde- und Benachrichtigungspflicht des § 109a Abs. 1 TKG wird den Diensteanbietern in § 109a Abs. 3 TKG und Art. 33 Abs. 5 DSGVO auferlegt, ein Verzeichnis über die meldepflichtigen Vorfälle zu führen. Darin sind sämtliche Vorfälle 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 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 bspw. der Fall sein, wenn ein Nutzer durch Schadsoftware auf seinem Computer Teil eines sog. „Botnetz“ geworden ist. Betroffene Computer können dann bspw. dazu verwendet werden, um ohne Wissen ihrer Besitzer Spam-E-Mails zu versenden oder andere Systeme anzugreifen. Die Diensteanbieter sind in diesen Fällen gehalten, ihren Nutzern 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 betroffenen 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 Art. 10 GG,
- in der StPO,
- im Außenwirtschaftsgesetz und
- in Landespolizeigesetzen zur Gefahrenabwehr.

§ 110 TKG regelt demgegenüber die technische Umsetzung der Überwachungsmaßnahmen. Gleichzeitig ermächtigt § 110 Abs. 2 TKG die Bundesregierung, eine Rechtsverordnung – die TKÜV – zu erlassen (siehe Anhang 8), die u. a. folgende Sachverhalte beinhaltet:

- Anforderungen an die technischen Einrichtungen sowie an die organisatorische Umsetzung von Überwachungsmaßnahmen mittels dieser Einrichtungen,
- Protokollierung der Umsetzung von Maßnahmen und Auskünften einschließlich der Kontrolle der Protokolle,
- 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 ggü. jedermann anbieten, technische Einrichtungen zur Umsetzung der gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und vorbereitende organisatorische Vorkehrungen hierfür 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 gespeicherte Verkehrsdaten, als auch über aufgrund von § 113b TKG gespeicherte Daten (Vorratsdatenspeicherung).

Die 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 (siehe 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 (siehe Kapitel 2.20).

Konkret sind gemäß § 111 Abs. 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 1. 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 sog. Anti-Terror-Gesetzgebung. Die BNetzA 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 öffentlich zugängliche Telekommunikationsdienste erbringt, 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 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen.

Die Auskünfte sind den Bedarfsträgern jederzeit 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.

§ 112 TKG erlaubt eine komplexe 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 KDAV und der TR AAV geregelt.

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 Abs. 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 umfassende Datenschutzkontrolle ermöglichen. Ruft die BNetzA Daten für die Polizei eines Bundeslandes ab, kann die zuständige Landesdatenschutzaufsichtsbehörde bei der Polizei kontrollieren, ob die Abfrage zulässig war. Die BNetzA wiederum wird von dem BfDI hinsichtlich der datenschutzrechtlichen Verpflichtungen kontrolliert. Im Gegensatz zu dem Verfahren nach § 113 TKG dürfen die Anbieter für Abfragen nach § 112 Abs. 5 S. 3 TKG den Bedarfsträgern und der BNetzA keine Kosten in Rechnung stellen.

2.21 Manuelles Auskunftsverfahren

Neben dem automatisierten Auskunftsverfahren sind die Diensteanbieter auch verpflichtet, manuelle Auskunftsersuchen von Sicherheitsbehörden zu beantworten. Die Auskunftspflicht bezieht sich dabei auf die nach den §§ 95 und 111 TKG erhobenen (Bestands-)Daten (siehe Kapitel 2.5 und 2.19). Zwar wurde § 95 TKG weitgehend von der DSGVO verdrängt, an den zu beauskunftenden Daten ändert dies jedoch nichts.

Bestandsdatenauskunft und Doppeltürenmodell

§ 113 TKG verpflichtet Telekommunikationsdiensteanbieter, Auskunftsersuchen berechtigter Stellen über Bestandsdaten zu beantworten. So müssen bspw. Name und Anschrift des Inhabers einer konkreten Rufnummer herausgegeben oder 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, soweit die besonderen gesetzlichen Voraussetzungen vorliegen (§ 100j Abs. 1 S. 2 StPO).

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 StPO geregelt sind.

Berechtigte Stellen

§ 113 Abs. 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 Abs. 1 S. 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 usw. 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 Abs. 3 TKG benannten Stellen vorbehalten. (Private) Rechteinhaber können ein Auskunftsersuchen nicht auf diese Norm stützen und müssen stattdessen auf das Verfahren nach § 101 UrhG (siehe Kapitel 3.10) zurückgreifen.

Prüfpflichten der Telekommunikationsanbieter

§ 113 Abs. 2 S. 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 usw.) 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 nach aktueller Rechtslage zwei Behörden, zum einen der generell für die Kontrolle und Durchsetzung der Vorschriften des TKG zuständigen BNetzA und zum anderen nach § 115 Abs. 4 TKG dem BfDI. Dieser tritt dabei an die Stelle der sonst nach § 40 BDSG zuständigen Landesdatenschutzbehörden, denen grundsätzlich die Aufsicht über den gesamten nicht-öffentlichen Bereich obliegt. Aus

dieser klar geregelten Kompetenzabgrenzung folgt allerdings nicht, dass Telekommunikationsunternehmen ausschließlich der Datenschutzaufsicht des BfDI unterliegen. Eine Zuständigkeit des BfDI für diese Unternehmen nach § 115 Abs. 4 TKG besteht nur, soweit personenbezogene Daten zur geschäftsmäßigen Erbringung von Telekommunikationsdiensten verarbeitet werden. Die Verarbeitung z. B. von Beschäftigtendaten dieser Unternehmen oder personenbezogener Daten von „Nicht-Kunden", wie z. B. Interessentendaten oder Daten, die bei einer Gewinnspielaktion erhoben wurden, unterliegen der Aufsicht der zuständigen Datenschutzaufsichtsbehörden der Länder; eine Übersichtsliste findet sich im Anhang 10.

Kontroll- und Beanstandungsrecht

Anders als die BNetzA, die bspw. bei Gesetzesverstößen Bußgeldverfahren einleiten, Anordnungen treffen oder andere aufsichtsrechtliche Maßnahmen ergreifen kann, sind die Kompetenzen des BfDI bisher eingeschränkt. Zwar hat dieser die Aufgabe, Telekommunikationsdiensteanbieter zu kontrollieren, sollte er hierbei jedoch einen Verstoß gegen das TKG feststellen, so kann dieser nur ggü. der BNetzA beanstandet, nicht jedoch ein Bußgeld gegen den Anbieter verhängt werden. Aufgrund der klaren Vorgaben des europäischen Rechts hinsichtlich der Unabhängigkeit der Datenschutzaufsicht sind jedoch in diesem Bereich entsprechende Anpassungen zu erwarten. Anders verhält es sich bei Datenschutzverletzungen nach DSGVO. Hier verfügt der BfDI bereits jetzt über eigene Abhilfebefugnisse nach Art. 58 Abs. 2 DSGVO.

Beratungsfunktion und Beschwerderecht

Neben seiner Kontrollfunktion berät der BfDI die Unternehmen der Telekommunikationsbranche sowie die öffentlichen Stellen des Bundes in datenschutzrechtlichen Fragen, etwa bei der Einführung neuer Dienste und Angebote. Eine weitere wichtige Aufgabe liegt in der Bearbeitung eingehender Beschwerden von Bürgerinnen und Bürgern. Wer annimmt, bei der Erhebung, Verarbeitung oder Nutzung seiner persönlichen Daten durch einen Telekommunikationsdiensteanbieter in seinen Rechten verletzt worden zu sein, kann sich an den BfDI wenden (Art. 57 Abs. 1 Buchst. f DSGVO). Als unabhängige Beschwerdeinstanz mit den o. g. Kontrollbefugnissen geht der BfDI den Beschwerden nach

und unterrichtet die Betroffenen über das Ergebnis. Alle Eingaben werden vertraulich behandelt. Auf Wunsch der Betroffenen bleibt ggü. den Telekommunikationsunternehmen der Name ungenannt, jedenfalls, solange eine anonyme Bearbeitung des Anliegens möglich ist. Zudem veröffentlicht der BfDI seit 2019 einen Jahresbericht über seine Tätigkeit, der auch Beiträge aus dem Telekommunikationsbereich umfasst. Die Tätigkeitsberichte (die bis Ende 2018 im Zweijahrestakt erschienen) können auf der Website des BfDI abgerufen werden.

3 Sonstige bereichsspezifische Normen

3.1 Einwilligung

Personenbezogene Daten dürfen nur auf Grundlage einer Einwilligung der betroffenen Person oder einer sonstigen gesetzlich geregelten Grundlage verarbeitet werden (Art. 6 Abs. 1 S. 1 Buchst. a DSGVO).

Wenn eine Rechtsvorschrift den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die Einwilligung der betroffenen Personen nicht an. Soll eine Einwilligung Grundlage für eine Verarbeitung sein, ist Folgendes zu beachten:

- Die Einwilligung muss durch eine eindeutige bestätigende Handlung erfolgen und freiwillig sein;
- die betroffene Person ist vorher über Umfang und Tragweite ihrer Einwilligung aufzuklären (insbesondere über den Verarbeitungszweck und die verantwortliche Stelle);
- sie ist auch darüber zu informieren, was geschieht, wenn sie personenbezogene Daten nicht bereitstellt (z. B. dass Ansprüche verloren gehen können), soweit nach den Umständen des Einzelfalls erforderlich oder wenn sie dies verlangt.

Die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen, also frei von Zwang sein. Dabei ist auch zu berücksichtigen, ob sich die betroffene Person in einem besonderen Abhängigkeitsverhältnis (z. B. Arbeitsverhältnis) befindet oder ob aufgrund einer faktischen Situation (bspw. Monopolstellung desjenigen, der die Einwilligung einholen will) ein Zwang besteht.

Bei der Verarbeitung *besonderer Kategorien personenbezogener Daten* gemäß Art. 9 DSGVO (siehe Kapitel 2.1) muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

In Bezug auf Dienste der Informationsgesellschaft werden erhöhte Anforderungen an Einwilligungen von Kindern gestellt, die das 16. Lebensjahr noch nicht vollendet haben. Hier kann die Einwilligung nur durch den Träger der elterlichen Verantwortung oder mit dessen Zustimmung erteilt werden (Art. 8 Abs. 1 S. 2 DSGVO).

3.2 Übermittlung personenbezogener Daten in Drittländer

Datenverkehr zwischen den EU-Mitgliedstaaten und mit den Vertragsstaaten des Europäischen Wirtschaftsraums im Anwendungsbereich des Unionsrechts ist datenschutzrechtlich genauso zu behandeln wie inländischer Datenverkehr. Dahingegen müssen für Datenübermittlungen in Drittländer zusätzlich die besonderen Bedingungen des Kapitels V der DSGVO erfüllt sein.

Die DSGVO sieht folgende Fälle vor, in denen eine Drittstaatenübermittlung zulässig sein kann:

- Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DSGVO)
  Mit einem sog. Angemessenheitsbeschluss stellt die Kommission fest, wenn ein jeweiliges Drittland ein angemessenes Schutzniveau bietet. 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.
  Außerdem gilt: Die Angemessenheitsbeschlüsse, die die Kommission vor dem Geltungsbeginn der DSGVO getroffen hat, bleiben so lange in Kraft, bis sie durch einen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden (Art. 45 Abs. 9 DSGVO).
  Die Adäquanzentscheidung zum *EU-US Privacy Shield* basiert auf Verhandlungen zwischen der Europäischen Kommission und den USA. Sie führt dazu, dass bei den nach den Regeln des Privacy Shields zertifizierten Unternehmen seitens der EU ein angemesse-

nes 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.

- Datenübermittlung vorbehaltlich geeigneter Garantien
  Falls kein Angemessenheitsbeschluss der Kommission vorliegt, muss der Verantwortliche oder der Auftragsverarbeiter „geeignete Garantien" vorsehen. Zu Letzteren gehören bspw. verbindliche interne Datenschutzvorschriften oder Standarddatenschutzklauseln, die von der Kommission zuvor erlassen wurden. In diesem Fall bedarf es keiner gesonderten Genehmigung durch eine Aufsichtsbehörde (vgl. Art. 46 Abs. 2 DSGVO). Des Weiteren können „geeignete Garantien" auch in individuellen Verträgen bestehen, die allerdings einer Genehmigung durch die zuständige Aufsichtsbehörde bedürfen (Art. 46 Abs. 3 DSGVO).

- Ausnahmen
  Darüber hinaus kommt eine Datenübermittlung an einen Drittstaat auch bei abschließend aufgeführter und grundsätzlich eng auszulegender Ausnahmeregelung in Betracht (Art. 49 DSGVO). Dies ist z. B. der Fall, wenn die betroffene Person in die Datenübermittlung ausdrücklich eingewilligt hat oder die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist.

3.3 Auftragsverarbeitung

Viele Telekommunikationsunternehmen bedienen sich Dritter bei der Erbringung und Abwicklung ihrer Dienste. Entschließt sich ein Unternehmen zum Outsourcing von Tätigkeiten, die die Verarbeitung personenbezogener Daten beinhalten, muss es zahlreiche rechtliche, technische und organisatorische Voraussetzungen erfüllen. Art. 28 DSGVO regelt die sog. *Auftragsverarbeitung*. Beispiele für die Verarbeitung personenbezogener Daten im Auftrag sind der Betrieb eines Rechenzentrums oder eines Callcenters.

Werden dem Auftragnehmer personenbezogene Daten zu diesem Zweck überlassen, findet datenschutzrechtlich gesehen keine Über-

mittlung statt, da der Auftragnehmer nicht Dritter ist. Die Rechtmäßigkeit der Auftragsverarbeitung setzt vor allem voraus, dass

- der Auftraggeber einen schriftlichen Auftrag erteilt hat; Art. 28 DSGVO legt dabei detailliert fest, was genau schriftlich geregelt werden muss,
- der Auftragnehmer nur auf Weisung seines Auftraggebers tätig werden darf;
- zudem muss sich der Auftraggeber 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 ggf. an vertrauenswürdige Dritte (etwa unabhängige Sachverständige oder Wirtschaftsprüfungsgesellschaften, die kein eigenes Interesse an der Bewertung haben) zu delegieren. Letzteres kommt insbesondere dann in Betracht, wenn die Auftragsverarbeitung 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. Eine Auftragsverarbeitung ist auch außerhalb der EU und des Europäischen Wirtschaftsraumes möglich, wenn die besonderen Bedingungen für die Drittstaatenübermittlung erfüllt sind.

3.4 Bonitätsprüfung und Inkasso

Bonitätsprüfung

Die Bonitätsprüfung ist dem Vertragsschluss vorgeschaltet und dient dazu, die Zahlungsfähigkeit und Zahlungswilligkeit potentieller Kunden festzustellen. Abhängig von dem Ergebnis der Bonitätsprüfung wird dann ein Vertrag geschlossen oder nicht. Ein berechtigtes Interesse der Telekommunikationsanbieter, personenbezogene Daten zum Zwecke der Bonitätsprüfung zu verarbeiten, besteht nur in denjenigen

Fällen, in denen sie vorleistungspflichtig sind (Postpaid-Verträge). Erfolgt die Bonitätsprüfung und die daran anknüpfende Entscheidung über den Vertragsschluss ausschließlich automatisiert, ist Art. 22 DSGVO zu beachten. Danach dürfen besondere Kategorien personenbezogener Daten – etwa die rassische und ethnische Herkunft – nur mit Einwilligung verarbeitet werden. Zudem müssen betroffene Personen das Recht haben, ihren eigenen Standpunkt darzulegen – etwa durch Schilderung der für die Bonität sprechenden Gesichtspunkte, die im automatisierten Verfahren nicht berücksichtigt wurden.

Häufig führen Telekommunikationsdiensteanbieter die Bonitätsprüfung nicht selbst durch, sondern bedienen sich hierzu Auskunfteien. Auskunfteien sind Unternehmen, die Prognosen zum künftigen Zahlungsverhalten von Privatpersonen verkaufen. Grundlage hierfür sind personenbezogene Daten der betroffenen Person. Aufgrund dieser Daten wird das zukünftige Zahlungsverhalten prognostiziert und in einem Wahrscheinlichkeitswert ausgedrückt, was auch als Scoring bezeichnet wird. Dies ist unter den Voraussetzungen des § 31 Abs. 1 BDSG zulässig. In § 31 Abs. 2 BDSG ist festgelegt, wann die Nichtbedienung von Forderungen (z. B. aus einem Vertrag mit einem Telekommunikationsdiensteanbieter) in das Scoring einbezogen werden darf. Jedoch dürfen nur fällige Forderungen eingezogen werden,

- die durch rechtskräftige Urteile festgestellt worden sind,
- die in einem Insolvenzverfahren festgestellt und vom Schuldner im Prüfungstermin nicht bestritten wurden,
- die ausdrücklich anerkannt wurden,
- bezüglich derer mindestens zweimal schriftlich gemahnt wurde,
- die erste Übermittlung mindestens vier Wochen zurückliegt,
- auf die mögliche Berücksichtigung durch eine Auskunftei hingewiesen und die Forderung nicht bestritten wurde,
- bei denen das zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und
- die betroffene Person zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet wurde.

Bei anderen als den vorgenannten Forderungen, die von den Auskunfteien in das Scoring nicht einbezogen werden dürfen, besteht auch keine Veranlassung für Telekommunikationsdiensteanbieter oder Inkassounternehmen, diesbezügliche personenbezogene Daten an Auskunfteien zu übermitteln.

Inkasso

Telekommunikationsdiensteanbieter machen offene Forderungen aus den Geschäftsbeziehungen mit ihren Kunden häufig nicht selber geltend, sondern bedienen sich hierzu Inkassounternehmen. Zu diesem Zweck werden personenbezogene Daten der Kunden an das Inkassounternehmen übermittelt. Eine Übermittlung der zur Geltendmachung der Forderung erforderlichen personenbezogenen Daten ist unter den Voraussetzungen von Art. 6 Abs. 1 S. 1 Buchst. f DSGVO und § 97 Abs. 1 S. 3 TKG zulässig. Die Telekommunikationsdiensteanbieter haben ein berechtigtes Interesse an der Geltendmachung ihrer Forderungen. Auch die Geltendmachung rechtlich unsicherer Forderungen ist datenschutzrechtlich erlaubt. Ob die Telekommunikationsdiensteanbieter die Forderungen selber geltend machen oder hierzu auf ein nach dem Rechtsdienstleistungsgesetz registriertes Inkassounternehmen zurückgreifen, ist ihre unternehmerische Entscheidung. Die Übermittlung personenbezogener Daten an Inkassounternehmen ist auch dann zulässig, wenn Kunden die Berechtigung der Forderung bestreiten. Aus dem Beschluss des BVerfG vom 14. August 2004 – 1 BvR 725/03 – wird allgemein geschlossen, dass die Beauftragung von Inkassounternehmen nicht nur mit schlichten Mahn- und Beitreibungstätigkeiten zulässig ist, sondern auch mit der Geltendmachung bestrittener Forderungen. Die Zulässigkeit der Übermittlung personenbezogener Daten an Inkassounternehmen hängt schließlich nicht davon ab, ob der Telekommunikationsdiensteanbieter die Kosten der Beauftragung des Inkassounternehmens von den Kunden erstattet verlangen kann.

Eingehendere Informationen zu diesem Thema finden Sie in der Veröffentlichungen „Datenverarbeitung in Inkassounternehmen – Antworten und häufig gestellte Fragen“ der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) unter www.ldi.nrw.de.

3.5 Widerspruchsrecht

Unter den Voraussetzungen von Art. 21 DSGVO bzw. § 95 Abs. 2 S. 2 TKG können Betroffene einer an sich rechtmäßigen Verarbeitung ihrer personenbezogenen Daten widersprechen. Hierauf sind sie von den Verantwortlichen hinzuweisen.

Bei Verarbeitungen zum Zwecke der Direktwerbung nach Art. 6 Abs. 1 S. 1 Buchst. f DSGVO bzw. § 95 Abs. 2 S. 2 TKG (siehe Kapitel 2.5) besteht das Widerspruchsrecht voraussetzungslos. Geworben werden darf dann nur noch ohne Rückgriff auf personenbezogene Daten. Faktisch führt dies in vielen Fällen dazu, dass die Werbung gänzlich unterbleibt. Dies liegt daran, dass verbreitete Werbeformen (z. B. per E-Mail, SMS oder postalisch) ohne Verarbeitung personenbezogener Daten nicht möglich sind.

Verarbeitungen zu anderen Zwecken auf der Grundlage von Art. 6 Abs. 1 S. 1 Buchst. e oder f DSGVO kann nur aus Gründen widersprochen werden, die sich aus der besonderen Situation der widersprechenden Person ergeben. Erforderlich ist, dass die widersprechende Person aus der Masse der betroffenen Personen, hinsichtlich derer die Verarbeitung zulässig ist, herausragt. Voraussetzung hierfür ist, dass ihre personenbezogenen Daten einen erhöhten Schutzbedarf erfordern, der der an sich zulässigen Verarbeitung in der konkreten Konstellation entgegensteht. In diesen Fällen muss der Widerspruch begründet werden. Im Falle eines begründeten Widerspruchs verarbeitet der Verantwortliche die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Bei Verarbeitungen, die auf anderen Rechtsgrundlagen als auf Art. 6 Abs. 1 Buchst. e oder f DSGVO bzw. § 95 Abs. 2 S. 2 TKG erfolgen, besteht grundsätzlich kein Widerspruchsrecht.

3.6 Information betroffener Personen nach Artikel 13 und 14 DSGVO

Wenn personenbezogene Daten erhoben werden, sind die hiervon betroffenen Personen zu informieren. Hierdurch soll die Transparenz der Datenverarbeitung sichergestellt werden.

Die Information erfolgt zum Zeitpunkt der Erhebung, sofern die Erhebung bei der betroffenen Person selbst erfolgt. Andernfalls hat die Information innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, spätestens aber innerhalb eines Monats zu erfolgen. Sollen personenbezogene Daten der Betroffenen zur Kommunikation mit diesen verwendet werden, sind sie spätestens bei der ersten Kontaktaufnahme zu informieren. Ist die Offenlegung ihrer Daten an einen anderen Empfänger beabsichtigt, sind sie spätestens bei der ersten Offenlegung zu informieren. Die Information muss umfassen:

- Name und Kontaktdaten der verantwortlichen Stelle (Firma, Anschrift),
- Kontaktdaten des Datenschutzbeauftragten, sofern einer benannt wurde,
- die Art der verarbeiteten personenbezogenen Daten, sofern deren Erhebung nicht bei der betroffenen Person erfolgte,
- die Zwecke und Rechtsgrundlagen der Verarbeitung,
- die Empfänger oder Kategorien von Empfängern, sofern eine Übermittlung an Dritte erfolgt,
- sofern eine Übermittlung personenbezogener Daten an Empfänger in Drittländer beabsichtigt ist, auch Informationen hierzu, insbesondere zum dortigen Datenschutzniveau bzw. den getroffenen Schutzvorkehrungen.

In bestimmten, im Gesetz genannten Fällen erfolgt keine Benachrichtigung, etwa weil eine überwiegende Geheimhaltungspflicht besteht, die Unterrichtung einen unverhältnismäßigen Aufwand erfordert oder der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat (Art. 13 Abs. 4; 14 Abs. 5 DSGVO sowie §§ 29, 32, 33 BDSG).

3.7 Auskunftsanspruch betroffener Personen

Das Datenschutzrecht stellt denjenigen, deren personenbezogene Daten durch Dritte verarbeitet werden, Instrumente zur Verfügung, um ihr Recht auf informationelle Selbstbestimmung wahrzunehmen. Art. 15 DSGVO regelt das Auskunftsrecht der 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 zu seiner Person gespeicherten Daten. Das TKG selbst enthält keine spezielle Vorschrift zum Auskunftsrecht, so dass hier die DSGVO 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. Art. 15 DSGVO spricht hier von Empfängern oder Kategorien von Empfängern. Der Begriff des Empfängers umfasst nicht nur Dritte außerhalb der verantwortlichen Stelle, sondern auch Auftragsverarbeiter. 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 Auskunfteien oder andere geschäftsmäßige Datenverarbeiter etc. Darüber hinaus kann Auskunft über den Zweck der Speicherung verlangt werden, d. h. die betreffende Verwaltungsaufgabe oder den speziellen Geschäftszweck.

Wie erhält man Auskunft?

Die Datenschutzerklärung der Telekommunikationsdiensteanbieter enthält üblicherweise Kontaktadressen, an die datenschutzrechtliche Anliegen wie der Auskunftsantrag adressiert werden können. Bei telefonischen Auskunftsanträgen ist eine sichere Identifizierung meist nicht möglich, so dass Betroffene in diesen Fällen auf andere Kommunikationskanäle verwiesen werden können. Es empfiehlt sich deshalb, die Auskunft von vornherein schriftlich oder elektronisch zu beantragen und anzugeben, welche Informationen konkret gewünscht werden. Beispiel: „Meine Daten im Zusammenhang mit meinem Festnetzanschluss“, aber nicht „Alles, was das Unternehmen über mich

hat“. Eine Kopie des Antrags sowie Nachweise zu dessen Versendung sollten bis zur Auskunftserteilung aufbewahrt werden. Der Auskunftserteilung geht regelmäßig eine Legitimationsprüfung voraus, ob der Auskunftsantrag wirklich von der betroffenen Person gestellt wurde. Hierzu stellen Telekommunikationsdiensteanbieter den Antragstellern üblicherweise einige Fragen zu den in der Kundendatenbank hinterlegten Daten, die in dieser Kombination ausschließlich von der Person beantwortet werden können, deren Identität bestätigt werden soll. Sofern um Übersendung einer Kopie eines amtlichen Lichtbildausweises gebeten wird, sollte nachgefragt werden, welche Angaben aus dem Ausweis benötigt werden. Die nicht benötigten Angaben sollten geschwärzt werden. Zum eigenen Schutz sollten Ausweiskopien nicht per unverschlüsselter E-Mail versendet werden. Aus denselben Gründen können verantwortliche Stellen die Auskunft nicht per unverschlüsselter E-Mail erteilen. Die Auskunft ist innerhalb eines Monats zur Verfügung zu stellen, sofern die verantwortliche Stelle keine Gründe für eine Fristverlängerung geltend machen kann, Art. 12 Abs. 3 DSGVO. In komplexen Fällen kann diese Frist um max. weitere 2 Monate verlängert werden.

Was kostet eine Auskunft?

Grundsätzlich muss für die Auskunft nichts bezahlt werden. Etwas anderes gilt nur dann, wenn der Antrag offenkundig unbegründet oder – insbesondere im Fall häufiger Wiederholungen – exzessiv ist, was vom Verantwortlichen nachgewiesen werden muss. Wie bereits unter der Rechtslage vor der DSGVO ist eine einmal im Kalenderjahr beantragte Auskunft noch nicht als exzessiv anzusehen. Für jede weitere Auskunft kann jedoch ein angemessenes Entgelt verlangt werden. 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. Wird eine Kopie der personenbezogenen Daten verlangt, die Gegenstand der Verarbeitung sind, ist die erste Kopie kostenfrei.

Was tun, wenn die Auskunft verweigert wird?

Jeder hat grundsätzlich einen Anspruch auf eine vollständige Auskunft. Die Auskunft kann nur in den gesetzlich geregelten Fällen verweigert oder beschränkt werden (Art. 12 Abs. 5 S. 2 Buchst. b und Art. 15 Abs. 4 DSGVO sowie §§ 27, 28, 29, 30, 34 BDSG). Praxisrelevant ist hier insbesondere die Auskunftsverweigerung nach § 34 Abs. 1 Nr. 2 Buchst. b BDSG, wenn Daten nur aufgrund von Aufbewahrungsvorschriften gespeichert werden – etwa nach Vertragsende – und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Das Recht auf Erhalt einer Datenkopie kann auch insoweit verweigert werden, als hierdurch Rechte und Freiheiten anderer Personen beeinträchtigt würden. So kann bspw. der Ehemann als Vertragspartner keine Kopie der Call-Detail-Record-Daten verlangen, aus der hervorgeht, wann das von der Ehefrau genutzte Mobiltelefon bei welcher Mobilfunkzelle eingewählt war. Wer mit der erteilten Auskunft unzufrieden ist und meint, dass ihm eine weitergehende Auskunft zusteht, kann sich beim BfDI beschweren und/oder bei Gericht Klage gegen die auskunftspflichtige Stelle erheben.

3.8 Recht auf Löschung („Recht auf Vergessenwerden“)

Die DSGVO schließt ein Recht auf Vergessenwerden ein. Nach Art. 17 Abs. 1 S. 1 DSGVO kann die betroffene Person von dem Verantwortlichen verlangen, die sie betreffenden personenbezogenen Daten unverzüglich zu löschen. Aus dieser Norm leitet sich also ein direkter Anspruch ab. Spiegelbildlich hierzu ist im zweiten Halbsatz eine Löschpflicht vorgesehen, so dass der Verantwortliche auch antragsunabhängig verpflichtet ist, personenbezogene Daten unverzüglich zu löschen, sofern insbesondere einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig;

- die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung;
- die betroffene Person legt gemäß Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor;
- die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

Es gibt allerdings auch Ausnahmen von dem Recht auf Löschung (vgl. Art. 17 Abs. 3 DSGVO und § 35 BDSG). Die wichtigsten sollen im Folgenden sind:

- Wenn die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist, scheidet ein Recht auf Löschung aus. Bei Presseerzeugnissen ist also das Recht auf Löschung nicht ohne weiteres möglich. Aber auch hier gibt es Ausnahmen, so etwa wenn Veröffentlichungen auf falschen Informationen beruhen.
- Das Gleiche gilt, wenn die Verarbeitung zur Wahrnehmung einer Aufgabe, die dem Verantwortlichen übertragen wurde und im öffentlichen Interesse liegt, erforderlich ist. Dies ist regelmäßig bei Datenverarbeitungen durch Behörden der Fall, die im öffentlichen Interesse tätig werden. So kann z. B. für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke eine langfristige Speicherung erforderlich sein, so dass dann eine Löschung nicht verlangt werden kann.

Der Löschungsanspruch richtet sich auf die unverzügliche Löschung der betreffenden Daten. Wurden die Daten anderen ggü. offengelegt, muss der Verantwortliche diesen soweit möglich und zumutbar jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilen (Art. 19 DSGVO). Dahinter steht der Gedanke, dass es nicht Sache der Betroffenen ist, ihren Daten hinterherzulaufen, sondern sich derjenige, der die Daten in die Welt gesetzt hat, darum kümmern soll. Selbstverständlich können Betroffene trotzdem vom Verantwortlichen Unterrichtung über die Empfänger verlangen, so dass sie ihre Rechte den Empfängern ggü. ggf. selbst geltend machen können.

3.9 Recht auf Datenübertragbarkeit

Mit dem Recht auf Datenübertragbarkeit (auch Datenportabilität genannt) können betroffene Personen ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten. Der bisherige Verantwortliche muss die Daten unentgeltlich bereitstellen und darf die Betroffenen nicht daran hindern, die Daten an einen anderen Verantwortlichen zu übermitteln. Soweit technisch machbar, können Betroffene sogar verlangen, dass der bisherige Verantwortliche die Daten unentgeltlich an den neuen Verantwortlichen übermittelt. Hierdurch soll der Umzug von einem Dienst zum anderen erleichtert werden, wenngleich das Recht auf Datenübertragbarkeit nicht auf solche Umzugsfälle beschränkt ist.

Vom Recht auf Datenübertragbarkeit sind ausschließlich solche personenbezogenen Daten umfasst, die den Anspruchsinhaber selbst betreffen. Das trifft regelmäßig zu für Bestandsdaten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses erhoben wurden oder für Profildaten in einem sozialen Netzwerk. Handelt es sich dagegen um Datensätze ohne Informationen über die betroffene Person, besteht kein Anspruch auf Datenübertragbarkeit, weil es am Bezug zur betroffenen Person fehlt. Auch gilt das Recht auf Datenübertragbarkeit nicht für die Mitnahme von Rufnummern. Im Gegensatz zum Recht auf Datenportabilität darf die Rufnummernmitnahme deshalb auch etwas kosten. Vgl. hierzu auch die Sonderregelungen in § 46 TKG, die der Umsetzung von Art. 30 der RL 2002/22/EG dienen und der DSGVO insoweit vorgehen.

Art. 20 Abs. 1 DSGVO beschränkt das Recht auf Datenübertragbarkeit nicht auf solche Daten, die ausschließlich den Anspruchsinhaber und keine weiteren Personen betreffen (relevant etwa bei der Mitnahme selbst angelegter Kontaktverzeichnisse). Jedoch gilt dann in diesem Fall Art. 20 Abs. 4 DSGVO, wonach die Rechte und Freiheiten anderer Personen nicht beeinträchtigen werden dürfen.

Zusätzlich bezieht sich der Anspruch auf Datenübertragbarkeit nur auf solche Daten, die dem Verantwortlichen von der betroffenen Person bereitgestellt wurden. Dabei ist es allerdings nicht erforderlich, dass die Daten aktiv bereitgestellt wurden, etwa in einem Web-Formular. Vielmehr genügt es, dass die Daten durch Messungen oder Aufzeich-

nungen von Aktivitäten der betroffenen Person generiert wurden (z. B. durch einen Fitness-Tracker).

Das Recht auf Datenübertragung gilt immer dann, wenn die folgenden zwei Voraussetzungen erfüllt sind:

- Verarbeitung muss auf einer Einwilligung gemäß Art. 6 Abs. 1 Buchst. a oder Art. 9 Abs. 2 Buchst. a DSGVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 Buchst. b DSGVO beruhen und
- die Verarbeitung muss mithilfe automatisierter Verfahren erfolgen.

Ausgeschlossen ist das Recht auf Datenübertragbarkeit für Verarbeitungen, die für die Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 20 Abs. 3 S. 2 DSGVO). So kann nicht verlangt werden, dass die Daten von einer Behörde zu einer anderen Behörde übertragen werden.

Der Antrag kann in geeigneter Form, schriftlich, in Textform oder auch mündlich geltend gemacht werden. Der Beantragende muss jedoch seine Identität in geeigneter Form nachweisen können. Hat der Verantwortliche z. B. bei einem mündlich geäußerten Antrag begründete Zweifel an der Identität, kann er zusätzliche Informationen zur Bestätigung der Identität anfordern (Art. 12 Abs. 6 DSGVO). Schließlich kann er die Datenübertragung auch dann verweigern, wenn er die Datensätze der Betroffenen nicht finden kann.

Im Falle einer Ablehnung hat der Verantwortliche die Betroffenen auf ihre Beschwerdemöglichkeit bei der zuständigen Aufsichtsbehörde sowie die gerichtliche Klagemöglichkeit gegen den Verantwortlichen hinzuweisen.

3.10 Auskunftsansprüche nach § 101 Urheberrechtsgesetz

Im digitalen Zeitalter werden Musik- oder Filmdateien oft illegal verbreitet. Gegen diese Art der Urheberrechtsverletzung geht die Musik- und Filmindustrie als Rechteinhaber vor. Sobald ein Nutzer 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 Nutzer 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 Abs. 2 UrhG insbesondere das Recht eingeräumt, von den Internet-Zugangsprovidern Auskunft über die Identität des Rechteverletzers zu erhalten. Zur Geltendmachung des Auskunftsanspruchs wird zunächst die IP-Adresse des Rechteverletzers samt Datum und Uhrzeit benötigt. Die Rechteinhaber bzw. deren Anwälte bedienen sich hierzu 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.

Die Anwälte der Rechteinhaber stellen 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*). Denn da bei der Ermittlung der Identität des Rechteverletzers das Fernmeldegeheimnis betroffen ist, ist für die Auskunftserteilung eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten erforderlich (§ 101 Abs. 9 UrhG).

Die betreffenden Verkehrsdaten dürfen jedoch höchstens sieben Tage vom Internet-Zugangsprovider aufbewahrt 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 zuerst einmal verpflichtet, die betreffenden Verkehrsdaten bis zur gerichtlichen Gestattungsentscheidung aufzubewahren.

Stellt das Gericht fest, dass die Voraussetzungen des Auskunftsanspruches aus § 101 Abs. 2 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 des Betroffenen erhebt, muss gemäß Art. 14 DSGVO den Betroffenen über die Speicherung, die Art der Daten, die Zweckbestimmung und Rechtsgrundlagen der Verarbeitung und die Identität der verantwortlichen Stelle benachrichtigen. Sobald die Anwälte der Rechteinhaber die Daten der Internet-Zugangsprovider erstmalig erhalten, müssen sie also die Betroffenen hierüber innerhalb angemessener Frist, spätestens innerhalb eines Monats, informieren. Anwaltliche Verschwiegenheitspflichten stehen der Informationspflicht in der hier zu beurteilenden Konstellationen nicht entgegen. Anwälte können die Informationen anlässlich der Abmahnungen erteilen.

Betroffene, deren personenbezogene Daten von dem Internet-Zugangsprovider weitergegeben wurden, können bei ihrem Internet-Zugangsprovider Auskunft nach Art. 15 DSGVO verlangen. Hier ist jedoch zu beachten, dass sich das Auskunftsrecht ausschließlich auf personenbezogene Daten bezieht, die zum Zeitpunkt der Geltendmachung des Auskunftsrechts noch Gegenstand der Verarbeitung sind. Informationen dazu, welche IP-Adresse dem eigenen Anschluss zum Zeitpunkt der Urheberrechtsverletzung zugeordnet war, sind in der Regel bereits gelöscht und brauchen demzufolge nicht beauskunftet zu werden. Wie

bereits beschrieben, werden die hierzu erforderlichen Verkehrsdaten höchstens sieben Tage lang gespeichert. Von der Abmahnung erfahren Betroffene üblicherweise erst später. Das Schreiben des Internet-Zugangsproviders zur Auskunftserteilung an den Anwalt dürfte aber noch länger vorhanden sein, so dass hier vom Internet-Zugangsprovider eine Kopie verlangt werden könnte.

3.11 Auskünfte an Strafverfolgungsbehörden

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.

Auskunftsersuchen nach § 100g StPO

Nach **§ 100g Abs. 1 S. 1 StPO** dürfen zur Verfolgung bestimmter Straftaten von auch im Einzelfall erheblicher Bedeutung oder wenn eine Straftat mittels Telekommunikation begangen wird, Verkehrsdaten nach § 96 Abs. 1 TKG erhoben werden. Diese Daten müssen für die Erforschung des Sachverhaltes erforderlich sein. Die Erhebung der Daten muss ferner in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Wurde eine Straftat mittels Telekommunikation begangen, ist diese Maßnahme nur zulässig, wenn die Erforschung des Sachverhaltes auf andere Weise aussichtslos wäre. Die Erhebung von Standortdaten in Echtzeit ist bei diesen Straftaten nicht zulässig (§ 100g Abs. 1 S. 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 Abs. 1 S. 2 TKG erwähnten „anderen gesetzlichen Vorschriften“ und begründet eine Auskunftspflicht des Diensteanbieters (siehe 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 die Verfassungsmäßigkeit der Regelungen zur Verpflichtung geschäftsmäßiger Anbieter von Telekommunikationsdiensten geprüft hat, bestimmte Bestandsdaten zu speichern und diese im Wege des automatisierten oder manuellen Auskunftsverfahrens gemäß §§ 112 und 113 TKG zu beauskunften (siehe 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 (siehe Kapitel 2.5) und 111 (siehe 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 Abs. 3 StPO grundsätzlich eine richterliche Anordnung erforderlich. Schließlich ist in Abs. 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.

3.12 Telemediengesetz

Das 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

Der *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. Angebote 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 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 (siehe 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 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.

Datenschutzvorschriften für Telemedienangebote

Im *Abschnitt 4* des TMG finden sich Vorschriften zum Datenschutz bei Telemedienangeboten. Diese sind nach Ansicht der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder allerdings nicht mehr anwendbar. Seit Inkrafttreten der DSGVO ist diese als höherrangiges Recht anzuwenden. Bestehende nationale Regelungen sind nur dann weiter anwendbar, wenn die DSGVO dies ausdrücklich zulässt. Art. 95 DSGVO enthält eine solche Öffnungsklausel für Normen, mit denen die E-Privacy-Richtlinie umgesetzt wird. Dies ist beim TMG nach Ansicht der Datenschutzaufsichtsbehörden nicht der Fall. Anbieter müssen sich bei ihren Datenverarbeitungen auf eine Ermächtigungsgrundlage in der DSGVO stützen können. Hinsichtlich Cookies wird hier insbesondere Art. 6 Abs. 1 Buchst. f DSGVO relevant. Die Datenschutzkonferenz hat hierzu auch eine „Orientierungshilfe für Anbieter von Telemedien“ herausgegeben, in der weitere Einzelheiten hierzu nachzulesen sind.

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 Abs. 3 TMG). Allerdings enthält das TMG keine Regelung über die zuständige Verwaltungsbehörde, so

dass die allgemeinen Vorschriften des OWiG gelten. Nach § 36 Abs. 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 (siehe 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.

4 Praxisrelevante Aspekte

4.1 Telekommunikationsanlagen von Firmen und Behörden

Als Telekommunikationsanlage wird jedwede technische Einrichtung oder System verstanden, die Sprachnachrichten übertragen und vermitteln. Im Kontext von Behörden und Unternehmen werden diese Systeme eingesetzt, um mehrere Endgeräte (Telefon, Fax, PC etc.) direkt untereinander zu verbinden bzw. die Telekommunikationsanlage über ausgehende Leitungen mit öffentlichen Telekommunikationsnetzen zu verbinden.

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 jeder Teilnehmer einen separaten Zugang benötigt.

Weiterhin bietet eine Telefonanlage diverse nützliche Leistungsmerkmale wie z. B. das Weiterverbinden von Anrufen, die Bereitstellung von Sammelrufnummern, auch Rufum- und Rufweiterleitungen oder Konferenzschaltungen. Waren bis vor einigen Jahren überwiegend ISDN-basierte TK-Anlagen in Betrieb, sind heute überwiegend VoIP-Anlagen üblich. Im Zuge der technischen Fortentwicklung werden neben „schnurlosen Telefonen“ nach dem DECT-Standard auch stationäre und mobile Computer (APC, Laptops, Tablets etc.) als TK-Anlagen verwendet. Letztere bieten über zusätzliche Funktionen erweiterte Möglichkeiten der elektronischen Zusammenarbeit der Beschäftigten untereinander.

Nachfolgend werden die beim Betrieb von Telekommunikationsanlagen datenschutzrechtlich relevanten Themen erläutert sowie Hinweise gegeben, wie der Betrieb datenschutzkonform gestaltet werden kann; ergänzend sei auf das IT-Grundschutz-Kompendium und die Bausteine des BSI hingewiesen, welche auf dessen Website veröffentlicht sind.

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 in einem Programm die Integration der Funktionen einer TK-Anlage, auch mit Videokonferenzen, garniert mit einem Instant Messenger, der 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 dieselben sind. Beim Einsatz einer UC-Lösung sollte auf folgendes geachtet werden:

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 den Nutzern überlassen werden, sondern von vornherein durch den Administrator auf einen angemessenen Rahmen festgelegt werden; eine zusätzliche Löschmöglichkeit für Rufnummernhistorien etc. durch die Nutzer selbst erscheint sinnvoll.

Präsenzinformation

Die meist nahtlose Integration der unterschiedlichen Medien- und Informationsquellen ermöglicht auch Ungeahntes. So etwa 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 stammen) 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.

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 modernen Telekommunikationsanlagen können gezielt Leistungsmerkmale für einzelne Nebenstellen freigegeben, oder aber auch gezielt gesperrt werden.

Das Gefährdungspotenzial von Telekommunikationsanlagen betrifft neben der Manipulation der Hardware und der Software auch die missbräuchliche Nutzung der vorhandenen Funktionalitäten. Hierzu gehört z. B. das Aufschalten auf bestehende Verbindungen, der unbemerkte Aufbau einer Dreierkonferenz, die Rufumleitung auf einen Fremdapparat oder das direkte Ansprechen eines Teilnehmers (Wechselsprechanlage). Diese oder ähnliche Leistungsmerkmale können – vorausgesetzt, entsprechendes Fachwissen ist vorhanden – zum Gebührenbetrug oder Abhören missbraucht werden.

Die Verhinderung des Missbrauchs dieser 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 befugtem Personal der Zugriff auf die Anlage und die zugehörigen Systemkomponenten erlaubt ist. In solche Überlegungen ist insbesondere auch die Zugriffsmöglichkeit per Fernwartung mit einzubeziehen. In diesem Zusammenhang sind die Publikationen des BSI (siehe Kapitel 2.16) zu beachten, die Hinweise zum sicheren Betrieb und (insbesondere für Behörden) zur Beschaffung von Telekommunikationsanlagen enthalten. Vor der Nutzung eines Leistungsmerkmals ist zu prüfen, ob ein Einsatz notwendig ist. Die zugehörige Entscheidung ist zu dokumentieren. Nicht benötigte Leistungsmerkmale sollten grundsätzlich deaktiviert werden. Manche Telekommunikationsanlagen verfügen über Ländereinstellungen, bei denen auch rechtliche Vorgaben für die verschiedenen Länder berücksichtigt sind. Es sollte darauf geachtet werden, in jedem Fall auch *„Deutschland“* zu aktivieren.

Anruflisten

Telekommunikationsgeräte verfügen heute in aller Regel 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 Nutzer 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 beschriebenen Komforts ist dies aus datenschutzrechtlicher Sicht im behördlichen und unternehmerischen Kontext eher kritisch zu sehen und daher zu reglementieren.

Die in den Anruflisten gespeicherten Informationen stellen Verkehrsdaten gemäß § 96 TKG dar (siehe Kapitel 2.6). Ist das Leistungsmerkmal *Anruflisten* verfügbar, so ist die Speicherung der Telefonnummern generell auf einen angemessenen zeitlichen Rahmen zu begrenzen. Dies sollte durch entsprechende Konfiguration der TK-Anlage zentral erfolgen. Im Sinne der Datenminimierung sollte auch überlegt werden welche Anrufliste für den Endbenutzer benötigt wird. Sollte diese Liste dezentral in den Endgeräten gespeichert werden, ist bei der Reparatur und Entsorgung der Geräte entsprechend sorgfältig vorzugehen.

Ergänzend zu diesen technischen Maßnahmen wird den Betreibern von TK-Anlagen empfohlen, alle 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 eine Taste gedrückt zu werden. Wird für solche Endgeräte das Leistungsmerkmal *„Direktansprechen/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/Chefin“ und Sekretariat eingerichtet, häufig wird es aber auch in Teamfunktion gewünscht: Der Chef/die Chefin kann damit kurze Rückfragen an seine/ihre 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 ist ein optisches und akustisches Signal zu erzeugen, welches dem Nutzer gestattet die Aktivierung zu erkennen. Sofern möglich ist das Leistungsmerkmal *„Ansprechschutz“* zur Verfügung zu stellen, welches ein Direktansprechen eines konkreten Anschlusses/Gerätes unterbindet.

Konferenzschaltung

Ähnliche Beeinträchtigungen der Persönlichkeitsrechte können sich auch bei *Konferenzschaltungen* ergeben. Nicht alle Telekommunikationsanlagen machen durch ein obligatorisches, nicht zu unterdrückendes Signal bzw. Darstellung deutlich, wenn ein neuer Teilnehmer in die Verbindung einbezogen wird oder wenn ein Teilnehmer die *Telefonkonferenz* verlässt. Wird kein automatisches Signal erzeugt oder ist die Darstellung fehlerhaft, wäre es z. B. möglich, dass 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 Teilnehmer 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 Abs. 1 Nr. 1 StGB sogar strafbar (siehe Kapitel 4.7). 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 Nachteilen ggü. den ausschließlich für Telefongespräche vorgesehenen Netzen verbunden.

Sicherheit

Die Verschmelzung und damit die Vereinheitlichung des Kommunikationsmediums bergen zusätzliche Gefahren. 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, 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 (siehe 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 verschlüsseltes 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 kostenfrei 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.

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.

Das Fax-Protokoll wurde für eine direkte Kommunikation ausgelegt, die bei analogen und ISDN-Telefonanschlüssen gegeben ist bzw. war. Bei VoIP kann es aber zu geringen Verzögerungen oder Paketverlusten kommen. Diese fallen beim Telefonieren nicht auf, können bei Faxen aber zu Abbrüchen führen. Eine der eingesetzten Methoden zur zuverlässigen Übertragung von Telefaxen bei VoIP-Anschlüssen besteht in der Umwandlung der Faxe in E-Mails. Fraglich ist dann allerdings, ob die Vertraulichkeit, die bei einer direkten Faxübertragung mit einem Telefonat vergleichbar ist, noch gegeben ist.

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.

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 USA begonnen, technische Einrichtungen von 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 SIP. Der TK-Anbieter hält dafür 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 Kunden müssen 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 wäre bei der Verwendung einer virtuellen Telefonanlage als grundsätzlich kritisch zu bewerten, wenn die Anbindung der Telefone an die Anlage unverschlüsselt über das Internet erfolgt. Das verwendete Protokoll SIP ist gegen unerwünschte Zuhörer nicht gerüstet und mit einfachsten Mitteln zu manipulieren. Beim Einsatz einer solchen Anlage kann z. B. ein verschlüsseltes VPN eingesetzt werden, auch eine Verschlüsselung von Inhalten und Signalisierung kommt in Frage. 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 EVN 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 Dauer des Gesprächs, Tarifangaben. 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 (siehe Kapitel 2.6) zu werten. Dabei sind die Vorgaben des TKG und/oder der DSGVO zu beachten. Nachfolgend werden zwei prinzipielle Betriebskonzepte (sowie die Kombination aus beiden Möglichkeiten) von TK-Anlagen betrachtet. 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 der DSGVO. Das Verbot zur privaten Nutzung kann z. B. durch geeignete Dienstanweisungen geregelt sein.

Die Protokollierung der Verkehrsdaten soll sich gemäß Art. 5 Abs. 1 Buchst. c DSGVO am Grundsatz der Datenminimierung orientieren. 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 (z. B. Erstellung einer Statistik zur Verteilung der Gesprächskosten, aufgeteilt nach Abteilungen) sind diese so früh wie möglich zu anonymisieren (siehe Art. 5 Abs. 1 Buchst. e DSGVO). Weiterhin ist die Zweckbindung der erhobenen Verkehrsdaten zu beachten (siehe Art. 5 Abs. 1 Buchst. b DSGVO). Werden Daten zu Abrechnungszwecken erhoben, dürfen sie grundsätzlich nicht für weitere Zwecke genutzt werden. 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, dürfen personenbezogene Daten nur nach Weisung verarbeiten (siehe Art. 29 und Art. 32 Abs. 4 DSGVO bzw. § 52 BDSG) und müssen ggf. zur Wahrung des Datengeheimnisses verpflichten werden (§ 53 BDSG). Dies ist durch den Verantwortlichen in geeigneter Form nachzuweisen (Rechenschaftspflicht; siehe Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO). 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 oder unrechtmäßig zu nutzen.

Dem Betreiber der TK-Anlage obliegt die Pflicht, technische und organisatorische Maßnahmen vorzusehen, die notwendig sind, um die TK-Anlage entsprechend den Anforderungen der DSGVO zu betreiben (siehe Kapitel 2.16). So ist z. B. der Zugriff auf die TK-Anlage zu schützen um unerlaubte Zugriffe und Manipulationen möglichst auszu-

schließen. Hierbei ist auf den Stand der Technik zurückzugreifen, der durch das BSI veröffentlicht wird.

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 z. B. 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 Nutzer erhoben wird. Der Betreiber der TK-Anlage ist ein Telekommunikationsdienstanbieter mit der Folge, dass neben der DSGVO auch 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 (siehe Kapitel 2.7). Wenn Daten für eine Störungsbeseitigung benötigt werden, dürfen diese ohne konkreten Anlass nur bis zu sieben Tage gespeichert werden (siehe 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 der DSGVO, dem BDSG und dem 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. Auf eine etwaige Protokollierung der Verarbeitungsvorgänge gemäß § 76 BDSG ist zu achten.

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 RL ist es, den wirtschaftlichen Betrieb von TK-Anlagen im behördlichen Umfeld zu regeln. Nach diesen Vorgaben ist grundsätzlich nur die dienstliche Nutzung von TK-Anlagen zulässig. Eine private Nutzung kann zugelassen werden, wobei die entstehenden Kosten der geführten Privatgespräche durch die Nutzer 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 grundsätzlich erhoben und gespeichert werden, wenn die Gesprächsgebühren in ein öffentliches Telefonnetz pauschal abgegolten werden (sog. *Flatrate-Tarife*). Stichproben können zur Abrechnung und zur Sicherstellung der Qualitätskontrolle erhoben werden, insbesondere wenn über die bestehenden Telefonkanäle des Regierungsnetzes hinaus auf kostenpflichtige Verbindungen umgeschaltet werden muss, um das Aufkommen zu bewältigen. Bei der Datenerhebung und -speicherung ist zwischen der Erfassung der dienstlichen Verbindungen und der privaten Verbindungen, – sofern gestattet – 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 Leistungs- und Verhaltenskontrolle eines Mitarbeiters).

Eine Besonderheit stellen in diesem Zusammenhang die Dienstanschlüsse der Personen dar, die aufgabenbezogen nicht der allgemeinen Dienstaufsicht unterliegen, wie z. B. Vertreter/Vertreterinnen des Personalrates oder die/der behördliche Datenschutzbeauftragte. Hier ist lediglich die Erhebung und Speicherung der Tarifeinheiten bzw. der Verbindungsentgelte zulässig, so dass die protokollierten Daten 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. Auch die Speicherung von Anruflisten in Endgeräten sollte beschränkt werden, insbesondere da hier auch externe Anrufe aufgelistet werden.

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 dem Nutzer 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 Privatgesprächen 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. Aufgrund der Verbreitung von Smartphones verliert die private Nutzung dienstlicher Anlagen für Telefonate ebenso wie die Kommunikation via E-Mails in der Praxis zunehmend an 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 heute neben Handys auch Smartphones, Notebooks oder Tablets mit Mobilfunkschnittstellen (Surfstick oder Steckplatz für SIM-Karte) 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, LTE und dem kommenden 5G. 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), der Latenzzeit und in den möglichen Datenübertragungsraten.

Im Gegensatz zur drahtgebundenen Telekommunikation wird die Sprach- und Datenübertragung bei der Mobilkommunikation per Funkanbindung realisiert. Dieses Übertragungsmedium ist physisch nicht abgesichert und die Inhalte müssen gegen mögliches Abhören und Manipulation geschützt werden. Daneben ist es bei großflächigen Mobilfunksystemen wie z. B. LTE oder verbundenen WLAN-Hotspots prinzipiell möglich, geografische Bewegungsprofile der Nutzer zu erstellen oder den aktuellen Standort zu bestimmen. Sofern die Geräte auch für weitere Dienste (Shopping, Streaming etc.) genutzt werden, lassen sich über die gewonnenen Daten weitere Profile zum Nutzerverhalten erstellen.

4.2.1 Drahtlose Kommunikation für die Telefonie im Festnetz

Bei der Nutzung von drahtlosen Geräten in der Festnetztelefonie findet in den mobilen Endgeräten eine Umwandlung der analogen Sprache zu digitalen Signalen und umgekehrt statt. Die Übertragung des digitalen Signals zwischen dem mobilen Endgerät und Basisstation wird technisch über Funkfrequenzen gelöst.

Als gängige technische Umsetzungen für die Übertragung sind DECT aber auch WLAN im Einsatz. Ein direktes Abhören des gesprochenen Wortes mit einfachen Funkempfängern ist durch die Digitalisierung zwar nicht möglich, der technische Aufwand für das Abfangen der Sig-

nale bei der Übertragung zwischen mobilem Endgerät und Basisstation ist hingegen mit vertretbarem Aufwand grundsätzlich realisierbar.

Sind die Inhalte nicht verschlüsselt übertragen worden, liegen sie in einem einfach zu transformierenden Format vor. Bereits im Jahre 2009 hat sich gezeigt, dass über DECT geführte Telefonate mit einem geringen Kostenumfang abgehört werden können. Dies war darin begründet, dass die meisten Hersteller damaliger DECT-Produkte wider besseres Wissen die optional für DECT standardisierte Verschlüsselung nicht in den Geräten vorsahen und/oder einsetzen. Auch wenn eine Verschlüsselung aktiviert ist, kann bei älteren Geräten (Basisstation als auch mobiles Endgerät) ein Verschlüsselungsalgorithmus verwendet werden, welcher nach heutiger Betrachtung als unsicher einzustufen ist. Für eine ungesicherte oder unzureichend abgesicherte WLAN-Verbindung gilt ähnliches (siehe Kapitel 4.4.5).

Für DECT ist die Weiterentwicklung CAT-iq verfügbar. Diese Technologie unterscheidet sich nicht maßgeblich vom Vorgänger, bietet allerdings einige Veränderungen hinsichtlich Anwendungsmöglichkeiten und Sicherheit. Eine Verschlüsselung ist ab CAT-iq Version 2.0/2.1 zwischen der Basisstation und dem mobilen Endgerät verpflichtend. Hierbei kann auf eine AES-Verschlüsselung zurückgegriffen werden, wobei für höhere Sicherheitsansprüche eine AES-Verschlüsselung mit 128 Bit erforderlich ist. Hier müsste man ggf. den Hersteller befragen. Darüber hinaus können die Geräte über die Internetanbindung deutlich einfacher mit einem Firmware-Update versorgt werden. Eine zeitnahe Schließung von Sicherheitslücken mittels Einspielung von Patches kann damit realisiert werden.

4.2.2 Mobilnetze und Endgeräte

Kaum eine Technik in der Kommunikation hat sich in den letzten Dekaden so rasant entwickelt wie der Mobilfunk. Galt in den Anfangsjahren zunächst der analoge Mobilfunk sowie der damalige Standard GSM noch als weitgehend sicher ggü. unerwünschten Zuhörern, so hat sich dies in den letzten Jahren stark verändert.

GSM

In den Mobilfunknetzen nach dem GSM-Standard (Standard 2. Generation) werden Sprache und Daten digital übertragen. Die digitalen

Daten werden für die Übertragung verschlüsselt. Der verwendete kryptographische Algorithmus als auch die Schlüssellänge entsprechen jedoch nicht mehr dem Stand der Technik, sodass ein Mithören eines Gespräches nicht ausgeschlossen werden kann. Eine weitere Angriffsmöglichkeit besteht durch eine „gefälschte" Basisstation (einem sog. IMSI-Catcher) eines Angreifers, in die sich ein GSM-Endgerät einbucht.

UMTS

Der Nachfolger UMTS (Standard 3. Generation) bringt hier bedingt Abhilfe. Bisher gelang es zwar, die Verschlüsselung bzw. die Sicherheitsaushandlungen von UMTS nur unter Laborverhältnissen zu unterwandern, eine praktische Anwendung für ein direktes Mithören ist jedoch schwer umsetzbar. Ein Mitschneiden der übertragenen Signale und darauffolgende Entschlüsselung ist jedoch denkbar.

UMTS-Endgeräte bieten auch eine Funktion, die sie weiterhin anfällig macht. Sollte die Versorgung mit UMTS nicht sichergestellt sein, kann fast jedes UMTS-Gerät auf den GSM-Standard zurückgreifen. Der zusätzliche Aufwand für das Blockieren des UMTS-Signals ist überschaubar, so dass die Angriffsmöglichkeiten auf GSM auch für UMTS-Endgeräte bestehen.

LTE (Advanced)

Der 4. Standard ermöglicht die paketbasierte Übermittlung von Telefonaten. VoLTE gilt noch als sicher, ist jedoch nicht flächendeckend verfügbar. Sofern das Gerät auf die zuvor genannten Standards zurückgreifen muss, liegen dieselben Sicherheitsrisiken vor. Auch zu LTE gibt es Informationen zu Sicherheitslücken, die darauf hinweisen, dass ein Einbuchen auf gefälschte Basisstationen und Umleitungen auf gefälschte Webseiten möglich ist.

5G

Mit dem 5. Standard der Mobilfunkgeneration sollen weitere datenschutzrechtliche und sicherheitstechnische Verbesserungen Einzug halten. Die Teilnehmeridentität (IMSI) soll nunmehr nur noch verschlüsselt übertragen werden. Ebenso soll auch ein Verbindungversuch mit falschen Mobilfunkstationen abgewehrt werden können. Die Übertragungskanäle zwischen den Providern werden nach Vorgabe des

5G-AKA-Protokolls abgesichert sein. Der Schutz der kommunizierten Inhalte wird sich hierdurch erhöhen.

Andererseits werden unterschiedliche Funktechniken angewandt, damit die Anforderungen an 5G erfüllt werden können. Hierfür ist eine Erweiterung des bisherigen Mobilfunknetzes notwendig. Da für 5G Frequenzen aus einem vergrößerten Frequenzbereich genutzt werden, müssen vor allem für den hochfrequenten Bereich zusätzliche Access Points aufgebaut werden. Der Standort eines Gerätes kann somit über 5G recht genau bestimmt werden, wenn die Verbindung über die relativ kleinen Funkzellen hergestellt wird, die in besonders hohen Frequenzbereichen arbeiten.

Solange kein flächendeckendes Netz zur Verfügung steht, wird ein Fallback auf die alten Generationen mit den jeweiligen Sicherheitslücken noch notwendig sein.

Endgeräte

Neben den Mobilfunkstandards manifestieren sich weitere Risiken auf den Endgeräten selbst.

Als Endgeräte sind heute vornehmlich Smartphones in Gebrauch. Die Hardware kommt von unterschiedlichen Anbietern aus unterschiedlichen Ländern. Hier sollte jeder für sich prüfen, welches Fertigungsland und welche Fertigungsweise akzeptiert werden kann.

Die Hardware wird gemeinhin mit vorinstallierter Software ausgeliefert. Je nach Hersteller werden unterschiedliche Betriebssysteme eingesetzt. Das einzelne Gerät wird mit einer Version des Betriebssystems ausgeliefert, welches über einen gewissen Zeitraum mit Softwareanpassungen (Patches) beliefert wird. Wenn der Hersteller die Bereitstellung der Softwareanpassungen beendet, kann das Gerät mit der installierten Software weiterhin eingesetzt werden, die Sicherheitslücken des veralteten Betriebssystems werden durch den Anbieter jedoch nicht mehr geschlossen.

Da man datenschutzrechtlich an die Software auf den Geräten mindestens die Forderung stellen sollte, möglichst auf dem neuesten Stand zu sein und den unbefugten Zugriff zu erschweren, sind noch die beiden Ebenen *Betriebssystem* und *Applikationen* näher zu betrachten (siehe 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 (siehe 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 einige 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 als praktische 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 unterzuschieben, bei dem das Display keine Aktivität anzeigt, obwohl die Raumgespräche abgehört werden. Es ist daher ratsam, bei wichtigen persönlichen Gesprächen das mobile Endgerät auszuschalten.

Schnittstellen

Mobile Endgeräte dienten in der Vergangenheit primär zum Telefonieren. In der Gegenwart werden auf den Geräten Adressen und Termine gespeichert und nehmen über verschiedene Schnittstellen Verbindung mit anderen Geräten in der näheren und weiteren Umgebung auf. Über diese Schnittstellen wird ein Austausch von Kontaktdaten, Shopping und Online-Banking oder auch Videostreaming ermöglicht. Jede aktive Schnittstelle bietet Angriffsmöglichkeiten. Auch wird eine Ortung des Geräts ermöglicht. Schnittstellen wie Bluetooth oder WLAN sollten daher generell nur anlassbezogen aktiviert werden und nach der Nutzung wieder deaktiviert werden.

Die technische Umsetzung erfolgt über Netzwerkadapter. Diese technischen Bauteile werden herstellerseitig mit einem eindeutigen Identifikationsmerkmal (MAC-Adresse o. Ä.) ausgeliefert. Aus diesem Identifikationsmerkmal lässt sich der Hersteller herauslesen, was wiederum Rückschlüsse auf den Hersteller des mobilen Endgeräts und des Betriebssystems zulässt. Wird der Adapter nicht deaktiviert, kann bei automatischer Einwahl in unterschiedliche WLANs ein Bewegungsprofil des Gerätes und somit des Nutzers erstellt werden.

4.2.4 Ortung bei Telemedien

In Kapitel 2.8 wurde die Rechtslage erläutert, unter welchen Voraussetzungen die Standortdaten von einem Telekommunikationsnetz oder Telekommunikationsdienst erhoben bzw. verwendet werden. Eine Standortbestimmung ist bei modernen Endgeräten, insbesondere Smartphones, direkt möglich, da viele Geräte eine recht exakte Bestimmung des Standortes via GPS und WLAN unterstützen. Werden diese Daten für Telemedien verwendet, wie z. B. bei Apps oder Webseiten, findet das TKG keine Anwendung.

Im TMG gibt es – im Unterschied zum TKG – keine besonderen Regelungen für die Nutzung von Standortdaten. Die DSGVO stellt zwar fest, dass Daten, die mittels Standortdaten einer Person zugeordnet werden können, als personenbezogen angesehen werden müssen, spezielle Regelungen für Standortdaten werden allerdings nicht getroffen.

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 den Mitgliedern einer Gruppe der Standort der anderen Mitglieder auf einer Karte angezeigt wird. 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 Daten oft über einen unbekannten Zeitraum gespeichert werden. Somit können Bewegungsprofile entstehen, die

wiederum mit anderen Daten verknüpfbar sind. Daher ist es wichtig, die Datenschutzerklärung durchzulesen und eine bewusste Entscheidung für oder gegen eine App zu treffen, bevor man eine Installation vornimmt. Gesundes Misstrauen ist ratsam, da manche Datenschutzerklärungen oder auch 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 Funktionen zur Standortermittlung (GPS, WLAN) zu deaktivieren und sie nur bei Bedarf einzuschalten. Auch sollten die App-Berechtigungen geprüft und ggf. angepasst werden, denn nicht jede App, die Standortdaten einfordert, muss diese auch bekommen. Weiterhin sollten auch die Datenschutz-Einstellungen des Betriebssystems selbst betrachtet und zum Schutz der eigenen Privatsphäre datenschutzfreundlich gewählt werden.

4.2.5 Kurznachrichten

Bei einem Telefonat können Anrufende bestimmen, ob die Rufnummer übertragen wird oder nicht (siehe Kapitel 2.12). Bei SMS wird die Rufnummer immer übertragen. Dies mag Smartphone-Besitzern, die diesen Dienst nur gelegentlich nutzen, nicht bewusst sein und kann somit zu einer ungewollten Weitergabe der Mobilfunknummer führen.

Eine SMS kann auch mit dem PC über das Internet versandt werden. Auf diesem Wege können auch anonyme Mitteilungen übermittelt werden. Eine SMS ist – wie auch eine Postkarte – nicht immer zurück verfolgbar. 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 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 näher erläutert.

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 dem Nutzer die Möglichkeiten eines Telefons zur Verfügung. Nur gemeinsam mit einer Mobilfunkverbindung kann das Hosentaschenrechensystem als Smartphone funktionieren.

Eine grundlegende Aufgabe des Betriebssystems ist es, den auf dem System installierten Apps 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 Apps auf die Daten und Funktionalitäten des Smartphones.

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 Apps 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. Aber solche Prüfungen können nicht zu hundert Prozent ausschließen, dass Apps keinen Schadcode beinhalten oder datenschutzkonform ausgestaltet sind. 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 und Nutzung nicht aus den Augen gelassen werden.

Problematisch ist der teils schwer kontrollierbare Datenfluss. So können bei bestimmten Betriebssystemumgebungen Apps z. B. auf das Telefonbuch zugreifen, ohne dass 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 Apps eingefordert wird. Der Zugriff muss deutlich sichtbar und nachvollziehbar für den Nutzer vom Betriebssystem geregelt werden. Zudem muss der Nutzer 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.

Die folgenden Aspekte sollten bei der Entwicklung und Nutzung unter allen Umständen berücksichtigt werden:

- Transparenz ggü. dem Nutzer durch geeignete Dialoge,
- Aufklärung der 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 oder technischen Erläuterungen,
- Aufklärung der Nutzer über eventuelle Übermittlung von Daten z. B. an Werbenetzwerke oder soziale Netzwerke und

→ uneingeschränkte Kontrolle des Nutzers über die Interaktion der App mit den Ressourcen und Datenzugriff bzw. -speicherung nur nach Notwendigkeit.

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.

Verantwortung des Nutzers

Die Verantwortung für einen sicheren Betrieb des Endgerätes liegt auch beim Nutzer. So sollten Sicherheitsupdates zeitnah eingespielt und Apps nur von vertrauenswürdigen Quellen geladen werden. Zudem sollten die Datenschutzerklärungen aufmerksam gelesen 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. kurzzeitigen Massenverkehrs-Dienste, beginnend mit 0137.

Die kostenlosen Gespräche über eine 0800-er Rufnummer dürfen nicht auf dem EVN des anrufenden Anschlussinhabers aufgeführt werden, da diese nicht entgeltrelevant sind. In Einzelfällen waren diese in der Vergangenheit dort dennoch verzeichnet, was bspw. 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 Premium-Rate-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 vom Anbieter zu tarifierten. 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 Abs. 3 TKG jedem Nutzer das Recht eingeräumt, von der BNetzA zu erfahren, welcher Anbieter sich hinter einer bestimmten Nummer verbirgt; nähere Informationen hierzu finden sich auf deren Website (www.bundesnetzagentur.de).

4.3.2 Premium-SMS

Premium-SMS können eingesetzt werden, um Zusatzleistungen (vorzugsweise in der Mobiltelefonie) zu buchen und zu bezahlen. Parkgebühren per SMS zahlen, Nachrichtendienste, Sportticker, Klingeltöne und Handy-Spiele und -Logos 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. Die TK-Provider sind nach

§ 45d Abs. 3 TKG verpflichtet Premium-SMS auf Wunsch des Kunden zu sperren.

4.3.3 Gesprächsvermittlung

Auch die Vermittlung zweier Gesprächsteilnehmer durch einen Anbieter, der nicht der Anschlussinhaber ist, wird als Mehrwertdienst bezeichnet. Beispiele sind die Rückruffunktion (engl.: Callback) und Callthrough. Hierbei sind zwei Fälle zu unterscheiden, bei denen jeweils eine zusätzliche Erhebung und Speicherung von Verkehrsdaten, Identifikationsmerkmalen etc. erfolgt, die man dem Dienstleister zur Verfügung stellt. Grundsätzlich sollte sich jeder Nutzer 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 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. Der Vorteil liegt in den geringeren Gebühren für ein Gespräch, insbesondere ins Ausland.

Callthrough

Auch beim sog. *Callthrough* werden zwei Gesprächsteilnehmer 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 dem gewünschten Teilnehmer auf und schaltet beide Teilnehmer 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, bspw. Computerviren, Trojaner und nicht zuletzt die Möglichkeit, jede einzelne Person mit allerlei Werbung zu behelligen, ob gewollt oder nicht. Insbesondere Online-Vermarkter und soziale Netze sammeln fleißig die Daten der Internetnutzer. Datenschutzrechtlich sind E-Mail-Dienste aufgrund des Urteils des EuGH vom 13.06.2019 (C-193/18) nicht mehr nach den Vorschriften des TKG zu bewerten; für andere Dienste der direkten Kommunikation gibt es aufgrund technischer Gegebenheiten einige Besonderheiten.

4.4.1 Internetzugang

Der Zugang zum Internet erfolgt in Deutschland in der Regel über Breitband-Datenfernübertragung (DSL etc.) oder mobile Verbindungen (LTE etc.). Für den Zugriff auf das Internet bedarf es dann eines Dienstleistungsvertrags mit einem Internet Service Provider (ISP). Erfolgt der Zugang über eine mobile Verbindung ist generell nur noch das internetfähige Endgerät notwendig. Im Heimbereich ist oft eine zusätzliche Hardwarekomponente (Router) notwendig um sich mit dem Dienst zu verbinden. Die Authentifizierungsmerkmale für den Dienst werden bei Vertragsabschluss ausgehändigt oder sind in den überlassenen Hardwarekomponenten bereits vorkonfiguriert.

Wird der Zugangspunkt und die Hardware übernommen, wie bei einer Vertragsübernahme von einem Vormieter, sollten diese Daten neu vergeben werden. Bei einem Verkauf von eigenen Hardwarekomponenten ist darauf zu achten, dass diese Daten vorab gelöscht werden. Oft dienen sie nämlich auch als Authentifizierungsmöglichkeit für den geschützten Kundenbereich im Internet, sodass mit den Zugangsdaten auch auf weitere personenbezogene Daten zugegriffen werden könnte.

Wird die Zugangskomponente im Netz angeschlossen wird der Teilnehmer angemeldet und erhält eine IP-Adresse aus dem Adressbestand. IP-Adressen, sowohl zeitlich stabil vergeben oder dynamisch zugeteilt, sind personenbezogene Daten, anhand derer die Anbieter die jeweiligen Kundinnen und Kunden identifizieren können. Die Zuordnung, welche IP-Adresse ein Nutzer zu einem bestimmten Zeitpunkt erhalten hat, wird in speziellen Logfiles gespeichert. Der 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 (siehe Kapitel 2.18 und 2.21). Auch bei vermuteten Urheberrechtsverletzungen wird ggf. auf diese Logfiles zurückgegriffen (siehe Kapitel 3.10).

Eine Sonderstellung im Bereich des Internetzugangs nehmen die sog. URLs ein. Beim Surfen gibt der Nutzer in seinem Browser eine bestimmte URL ein, die von einem DNS-Server in eine IP-Adresse umgesetzt wird. Auf diesem Wege wird der richtige Ort im Internet adressiert und der Nutzer erhält die gewünschten Daten. URLs können Hinweise auf die Interessen und Vorlieben des jeweiligen Nutzers geben. Oft reicht sogar die Angabe einer Website aus, 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 Abs. 1 TKG die Speicherung der Verkehrsdaten sowie von Steuerdaten informationstechnischer Protokolle, jedoch nicht von Inhaltsdaten. Ein Zeitraum von höchstens sieben Tagen wird aufgrund langjähriger Erfahrung als ausreichend angesehen (siehe Kapitel 2.10). Bei einer manuellen Erfassung oder Auswertung gibt es verschiedene Informationspflichten.

In § 109a Abs. 4 bis 6 TKG werden dem Netzbetreiber Maßnahmen zur Information des Nutzers sowie Umleitung des Verkehrs oder Sperrung des Anschlusses erlaubt, um Störungen zu beseitigen, die von Systemen des Nutzers ausgehen (siehe Kapitel 2.17). Dies ist für Fälle gedacht, bei denen ein Gerät (z. B. PC) des Kunden von Schadsoftware betroffen ist und andere Nutzer des Internets stört.

Viele Webseitenbetreiber nutzen kleine Textdateien, sog. Cookies, um die Telemedienangebote zu ermöglichen oder auch das Surfverhalten zu analysieren. Diese Textdateien werden vom Browser auf dem Endgerät des Nutzers gespeichert. In welchem Umfang der Browser Cookies speichert, kann mittels Browsereinstellungen von jedem Nutzer selbst reguliert werden. Etwa kann festgelegt werden, dass sog. Drittanbietercookies gar nicht erst angelegt werden. Ebenso kann die Speicherdauer der Cookies aktiv beeinflusst werden, indem bspw. beim Schließen des Browser sämtliche Cookiedaten gelöscht werden. Datenschutzrechtlich relevant ist in der Regel nicht der einzelne Cookie, sondern die mit dem Cookie verbundene Verarbeitung, die meist auf dem Server des Telemedienangebotes stattfindet. Liegt für die Verarbeitung eine Rechtmäßigkeit nach Art. 6 DSGVO vor, darf ein Cookie gesetzt und verarbeitet werden. Dies ist insbesondere bei der Bereitstellung von speziellen Funktionen (Warenkorb etc.), der Reichweitenmessung oder der Betrugsprävention gegeben.

Je nach Wahl und Einstellung des Browser kann jeder Nutzer sein Nutzungsverhalten im Web anonymisieren. Die meisten Browser speichern die besuchten Seiten in einer Chronik/Browserverlauf. Diese Daten können zur Erstellung/Vervollständigung von Nutzerprofilen verwendet werden und sollten zyklisch gelöscht werden. Einige Browser bieten hierzu auch eine automatisierte Löschung, die jeder Endbenutzer selbständig einstellen kann.

Auch Zugangsdaten zu Webseiten können in den Browsern gespeichert werden. Diese Funktionen bieten natürlich eine Nutzungserleichterung, ermöglichen jedoch auch das Ausspähen von Daten bzw. das Vervollständigen von Nutzerprofilen. Für die Speicherung von Passwörtern sollten man auf geeignetere Passwortprogrammen (Passwortsafes) zurückgreifen.

Für eine besonders sichere Verbindung z. B. für den Telearbeitsplatz, kann der zusätzliche Einsatz von VPN-Diensten notwendig sein. Mittels VPN-Dienst wird zunächst im physisch vorhandenen Netz ein eigenständiges logisches Netz erstellt. Die meisten VPN-Lösungen bieten auch eingebaute Verschlüsselungsmöglichkeiten, die in diesem Kontext eingesetzt werden müssen, um eine effektiven Schutz zu erreichen. Die im heimischen Bereich arbeitende Person kann dann über die gesicherte Verbindung auf das Firmennetz und die notwen-

digen Apps und Daten zugreifen. Die Teilnehmer der Kommunikation bleiben für einen potentiellen Angreifer ersichtlich, die Inhalte der Kommunikation sind jedoch verschlüsselt und nicht direkt abgreifbar.

Eine im Betrieb befindliche Zugangskomponente ist Teil des Netzwerkes und damit ein möglicher Ausgangspunkt einer Netzstörung. Erhält ein Dienstanbieter darüber Kenntnis, dass eine Störung von einem System des Endbenutzers ausgeht (z. B. Bot-Netz-Angriffe über gekaperte Router), ist er durch § 109a Abs. 5 TKG legitimiert, Maßnahmen zu ergreifen, um die Störung einzudämmen. Dies kann ggf. zur Abschottung des betroffenen Systems führen.

4.4.2 Internetnutzung in Hotels und Cafés

Die rechtliche Einordnung von WLAN-Diensten in Hotels und Cafés ist nur differenziert möglich. Eine Frage ist hier, ob es sich um eine geschlossene Benutzergruppe handelt oder ob das Angebot öffentlich zugänglich ist. Ebenfalls relevant ist, ob ein Dienst erbracht wird oder ob nur eine Mitwirkung erfolgt. Auch gibt es Anbieter, die für Hotels und Cafés spezielle WLAN-Angebote bereitstellen, die dem TKG und damit der Aufsicht des BfDI unterliegen. Eine abschließende Entscheidung der Rechtsgrundlage (TKG bzw. DSGVO) und Zuständigkeit ist jedoch nur im Einzelfall möglich. Zur Anwendbarkeit des TKG siehe auch Kapitel 2.2.

Oft hat ein Anbieter Bedenken, für eine missbräuchliche Nutzung rechtlich verantwortlich gemacht zu werden und speichert Daten zum Nutzer und zur Nutzung. Durch Rechtsänderungen bei der Störerhaftung sind für die Anbieter Rechtsfolgen weniger wahrscheinlich geworden. Insofern ist eine Protokollierung in Anbetracht des Gebots der Datensparsamkeit schwer begründbar. Im Einzelfall wäre zu entscheiden, ob z. B. eine Einwilligung für eine Protokollierung rechtlich ausreichend und zulässig wäre. In jedem Fall sollte man sich als Nutzer die Datenschutzregelungen und eventuelle Einwilligungen kritisch ansehen. Damit kann man meist schon erkennen, was über die Nutzung gespeichert wird.

4.4.3 Internetprotokollversionen

Die Verteilung der Datenpakete im Internet wird mithilfe des Internetprotokolls gewährleistet. Hierbei kommt sowohl die Version 4 (IPv4) als auch die Version 6 (IPv6) zum Einsatz.

Der Adressierungsbereich von IPv4 wurde in den Anfängen des Internets festgesetzt. Die knapp über vier Milliarden Adressen reichten 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 durch die Service Provider, die es ermöglichen, dass verschiedenen Endteilnehmern zu unterschiedlichen Zeiten eine IP-Adresse zugeteilt wird. Dies hat den aus Datenschutzsicht positiven Nebeneffekt, dass nicht jeder einzelne Nutzer direkt anhand der IP-Adresse erkennbar ist.

Die Umstellung des Protokolls auf die IPv6 wird sukzessive durchgeführt. Mit der Erweiterung des Adressraumes ändert sich auch die grundlegende Strategie der Adressverteilung. Es ist theoretisch zukünftig möglich, jedes an das Internet angeschlossene Gerät mit einer eigenen dauerhaften IP-Adresse zu versehen, quasi eine ID für jeden Computer, jedes Auto, jeden Kühlschrank und jeden Stromzähler.

Eine IPv6-Adresse besteht aus zwei gleich großen Teilen, *Präfix* und *Interface Identifier* genannt. Die Länge der IPv6-Adresse bewirkt, dass ein Nutzer 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 Nutzers 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 Nutzers bestimmt. Da nicht nur das Präfix datenschutz-

rechtlich bedeutsam ist, sind auch hier Maßnahmen gefragt, die den Adressbestandteil veränderlich halten. Der Standard zu IPv6 empfiehlt zu diesem Zweck den Einsatz der sog. *Privacy Extensions*. 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. Die Privacy Extension sollten entsprechend grundsätzlich aktiviert sein.

Neben der Privacy Extensions wurde auch IPSec als fester Bestandteil von IPv6 spezifiziert und für IPv4 nachspezifiziert. Mit IPSec kann eine verschlüsselte Übertragung der IP-Pakete, und somit der gesamten Kommunikation via IP-Netze, gewährleistet werden. Gemeinhin wird IPSec als technische Grundlage für den Aufbau von VPN-Verbindungen genutzt. Über diese Verbindungen kann auch eine verschlüsselte Übertragung von VoIP in eigenen Netzen ermöglicht werden.

4.4.4 Voice over IP

Sprache wird heute meist über das Internet-Protokoll, über VoIP, übertragen. Hier sind einige Fälle zu unterscheiden.

Bei Teilnehmern, die einen Internetanschluss und den Telefondienst in einem Paket vom gleichen Anbieter beziehen, ändert sich relativ wenig. Hier werden die IP-Pakete im DSL- oder Kabelrouter erzeugt und über den Internetanschluss zum Netzbetreiber übertragen. Wichtig ist hier, dass der Router eine aktuelle Firmware hat. Ansonsten bestehen keine grundlegenden Unterschiede zur früher üblichen Telefonie über ISDN.

Wenn man – im Router konfiguriert, per App im Smartphone oder mit einem PC-Programm – andere VoIP-Anbieter nutzt, z. B. um günstige Tarife ins Ausland zu nutzen, ist zu berücksichtigen dass die IP-Pakete über verschiedene Internetanbieter vom Anrufer bis zum VoIP-Anbieter weitergeleitet werden. Im Internet sind die Wege, über die ein Paket versendet wird, nicht sicher vorherzusehen. Besonders kritisch wird es, wenn unsichere Netze, z. B. von Hotels verwendet werden.

Eine Verschlüsselung ist zwar grundsätzlich möglich, wird aber nur bei bestimmten Diensten angeboten. Hier sind sowohl die Anbieter als auch die Hersteller von Routern und VoIP-Telefonen gefordert, eine

Verschlüsselung zu ermöglichen. Während beim Surfen meist schon https eingesetzt wird, besteht beim Telefonieren hier noch Nachholbedarf. Bei manchen Messengern (siehe Kapitel 4.6) ist eine verschlüsselte Sprachkommunikation möglich, insofern kann die Kommunikation sicherer sein, zumindest was die Inhalte der Kommunikation betrifft. Wie der Anbieter des Messengers die Verkehrsdaten, also z. B. der Information wann wer mit wem telefoniert hat, verarbeitet, sollte man aber dabei nicht aus dem Blick verlieren.

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. Dies führt dazu, dass die Rufnummernunterdrückung nicht oder nur unvollständig funktioniert. Unter Umständen kann sogar die gesamte von SIP übermittelte Protokollinformation angezeigt werden. Zudem kann bei ankommenden Anrufen die im Endgerät angezeigte Rufnummer manipuliert worden sein.

4.4.5 Wireless LAN (WLAN)

WLAN ermöglicht den Zugriff auf ein Kommunikationsnetz (Intranet/Internet) ohne die drahtgebundene Anbindung umständlich um- oder auszubauen. Ein Einbuchen in das Netz ist kabellos vom Sofa aus möglich. Auch in Unternehmen bietet diese Technologie eine Flexibilität hinsichtlich der Raum- und Arbeitsgestaltung. Für mobile Endgeräte bedeutet dies eine Befreiung von Steck- und Netzwerkdose.

Diese Freiheit wird durch Funktechnik ermöglicht. Die Informationen werden zwischen den Endgeräten und dem Access Point über die Luft übertragen. Was einen großen Komfort in der Nutzung gewährleistet, birgt jedoch auch Gefahren. Funkwellen breiten sich prinzipiell unkontrolliert und unbegrenzt aus. Ist ein Gebäude komplett mit der Funkinfrastruktur abgedeckt, 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. Eine Verschlüsselung der Verbindung ist daher ratsam. Zur Verschlüsselung stellen die meisten Geräte verschiedene Verfahren zur Verfügung. Von den gängig angebotenen Verfahren kann erst das WPA2-Verfahren als recht sicher angesehen werden. Sofern schon verfügbar sollte besser noch die neue

Version WPA3 genutzt werden. Wird der Access Point selbst betrieben, kann ggf. die Veröffentlichung des Netzwerknamens (SSID) unterdrückt werden. Der Netzwerkname selbst sollte auch keinen direkten Personenbezug zum Betreiber ermöglichen.

Öffentliche WLAN-Hot-Spots, wie zum Beispiel an Flughäfen oder Bahnhöfen, nehmen unter den Drahtlosnetzwerken einen Sonderstatus ein. Hot-Spots verfügen selten über ein Verschlüsselungsverfahren als Schutz gegen unbefugten Zugang oder Abhören und bieten somit jedem den Zugriff auf das drahtlose Netzwerk mit allen darin vorhandenen Daten. Man-in-the-middle-Attacken, bei denen durch geschickte Positionierung von Funkkomponenten echte Gegenstellen vorgegaukelt werden, und die z. B. die Datenübertragung zu bestimmten Netz-Segmenten protokollieren oder blockieren können, sind denkbar. Die Verwendung eines verschlüsselten Kanals (VPN) für alle Anwendungen bzw. einzelner verschlüsselter Verbindungen (https, SSL/TLS) sollte deswegen in dieser Konstellation obligatorisch sein.

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

WLAN wird auch von einigen Unternehmen zur Standortbestimmung genutzt. Über diese Standortbestimmungen können Bewegungsprofile erstellt werden. Sofern das WLAN nicht aktiv genutzt wird, sollte es an den Endgeräten deaktiviert und der Access Point (z. B. über Nacht) ausgeschaltet bleiben.

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 (siehe 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 Nutzenden 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.

Kostenfreie Tarife sind meist werbefinanziert. Oftmals wird 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. 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 SpamAngriffen. 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 unvorsichtige 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.

Nicht als Werbe-Mails zu klassifizieren sind sog. Display-Ads: Das OLG Nürnberg hat hierzu entschieden, dass es zulässig ist, in der Inbox von Freemailer-Kunden Werbeanzeigen einzublenden, die (nur) auf den ersten Blick so aussehen, als seien es E-Mails, letztlich aber klar als Werbung zu erkennen sind (Urteil vom 15.1.2019, Az. 3 U 724/18). Bei einer solchen Display-Ad handelt es sich nicht um eine E-Mail. Es macht also einen Unterschied, ob eine E-Mail von einem Absender an einen Empfänger gesendet und von dort abgerufen wird oder im Umfeld eines kostenfreien Postfachs im Internet Werbung geschaltet wird. In dem letzteren Fall ist keine Einwilligung des Kunden im Sinne des § 7 Abs. 2 Nr. 3 UWG erforderlich. Diese Art der Werbung ist daher zulässig.

4.6 Messenger-Dienste

Instant Messaging (englisch: „augenblickliche Nachrichtenübermittlung“) ermöglicht es nahezu in Echtzeit, Textnachrichten zwischen den Teilnehmern desselben Messenger-Dienstes oder interoperabler Messenger-Dienste zu übermitteln. Dabei erscheinen die Nachrichten quasi sofort auf dem Bildschirm des anderen Teilnehmers und

können von diesem auch umgehend beantwortet werden. Die Nutzung findet generell sowohl in einem direkten Verhältnis zwischen zwei Teilnehmern (Einzelchat) als auch in einem eingegrenzten Broadcast (Gruppenchat) statt. Die Kommunikationsinhalte können auch schnell von einem Teilnehmer an zunächst unbeteiligte Dritte weitergeleitet werden. Neben reinen Textmitteilungen können auch Dateien aller Art (Fotos, Video- u. Audiofiles, Word-Dokumente etc.) versendet werden. Einige Dienste bieten auch Sprach- und Videotelefonie an. Benötigt wird eine Software (App), die auf dem Endgerät (Smartphone, Tablet oder PC) installiert werden muss. Je nach Dienstanbieter ist auch das Hosten eines eigenen Servers für die Übermittlung der Daten und der Authentifizierung der Teilnehmer möglich.

Datenschutzrechtlich relevant sind neben dem Schutz des Kommunikationsinhaltes und der Bestandsdaten insbesondere die Zugriffsrechte, z. B. auf Kontaktlisten oder Standortdaten, die dem Messenger-Dienst eingeräumt werden. Des Weiteren sind die verpflichtend anzugebenden Bestandsdaten sowie die Konfigurationsmöglichkeiten zur Kennzeichnung von öffentlichen und privaten Informationen betrachtenswert.

Jeder Nutzer sollte sich vor Nutzung eines Messenger-Dienstes genau darüber informieren, wie der Messenger-Dienst-Anbieter die personenbezogenen Daten (Kommunikationsinhalte, Bestandsdaten) verwendet, schützt oder gar an Dritte weitergibt. Hier gibt es bezüglich des Schutzes Ihrer Daten sehr große Unterschiede.

Das TKG stammt aus einer Zeit, in der ausschließlich klassische Telekommunikationsanbieter das Angebot zur Telekommunikation stellten. Heute ersetzen die Messenger-Dienste zunehmend die klassische Telefonie. Als sog. OTT-Dienste unterfallen diese Angebote ebenfalls dem TKG und der DSGVO. Ausgehend vom Kodex elektronische Kommunikation (EU-Richtlinie 2018/1972) werden Messenger-Dienste künftig unter die E-Privacy Verordnung (vgl. Kapitel 1.6) fallen. Für diese Dienste werden nach heutigem Stand spätestens dann hoffentlich die gleichen strengen Vorgaben gelten wie für die klassische Telefonie.

4.7 Gesprächsaufzeichnung und Mithören

Gesprächsaufzeichnung

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

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

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

Eine Veröffentlichung von Mitschnitten aus dem Service-Center in Textform stellt eine zusätzliche Verarbeitung dar und benötigt eine gesonderte Einwilligung des Kunden.

Solche Mitschnitte gelten als personenbezogene Daten und unterfallen somit auch dem Auskunftsrecht nach Art. 15 DSGVO (siehe Kapitel 3.7) sowie dem Recht auf Löschung gemäß Art. 17 DSGVO (siehe Kapitel 3.8).

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. Dementsprechend verletzt das unerlaubte Mithören das Recht am gesprochenen Wort. Dieses Recht ist Teil des Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 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.

Stichwortverzeichnis

Anhang 1

Telekommunikationsgesetz (TKG)
– auszugsweise –

vom 22. Juni 2004 (BGBl. I S. 1190),
das zuletzt durch Artikel 319 der Verordnung vom 19. Juni 2020
(BGBl. I S. 1328) geändert worden ist

Inhaltsübersicht

Teil 5
Vergabe von Frequenzen, Nummern und Wegerechten

Abschnitt 2
Nummerierung

Teil 7
Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit

Abschnitt 1
Fernmeldegeheimnis

Abschnitt 2
Datenschutz

Abschnitt 3
Öffentliche Sicherheit

Teil 10
Straf- und Bußgeldvorschriften

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 behinderter 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. I S. 459), die durch Artikel 4 Absatz 21 des

Gesetzes vom 18. Juli 2016 (BGBl. I 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, Einstiegsschächte, 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 automa-

tisierten 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. 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 Kommunikation 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.

§ 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.

Teil 3
Kundenschutz

§ 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)[1] 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)[2] 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 Inan-

1 § 45d Abs. 2: Gem. Art. 5 Abs. 2 Satz 2 G v. 3.5.2012 I 958 (1717) mit dem Inkrafttreten einer Rechtsverordnung nach § 45n Abs. 1 i. V. m. Abs. 6 Nr. 1 (F. ab 3.5.2012) nicht mehr anzuwenden.

2 § 45d Abs. 3: Gem. Art. 5 Abs. 2 Satz 2 G v. 3.5.2012 I 958 (1717) mit dem Inkrafttreten einer Rechtsverordnung nach § 45n Abs. 1 i. V. m. Abs. 6 Nr. 2 (F. ab 3.5.2012) nicht mehr anzuwenden.

spruchnahme 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.

§ 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, für Bau und Heimat, 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,

5. über die Maßnahmen, die zur Gewährleistung der Gleichwertigkeit beim Zugang für behinderte Endnutzer getroffen worden sind, und
6. über die tatsächliche, standortbezogene Mobilfunknetzabdeckung, einschließlich einer Kartendarstellung zur aktuellen Netzabdeckung.

(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, für Bau und Heimat, 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. Die Bundesnetzagentur veröffentlicht auf ihrer Internetseite die von den Mobilfunknetzbetreibern übermittelten Informationen über die tatsächliche, standortbezogene Mobilfunknetzabdeckung einschließlich lokaler Schwerpunkte für Verbindungsabbrüche bei der Sprachtelefonie. 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 Individualvereinba-

rung 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.

Teil 5
Vergabe von Frequenzen, Nummern und Wegerechten

Abschnitt 2
Nummerierung

§ 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.

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. I 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 Herstellungsnum-

mer 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. 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 Teilneh-

mer, 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, für Bau und Heimat, 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. 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 Inneren, für Bau und Heimat 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 Telekommunika-

tionsdienste 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, § 51 Absatz 6 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 Personalausweisgetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes gilt § 8 Absatz 2 Satz 4 des Geldwäschegesetzes entsprechend. Für 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,
7. den Behörden der Zollverwaltung für die in § 2 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen sowie
8. den nach Landesrecht für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständigen Behörden für die in § 2 Absatz 3 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 Inneren, für Bau und Heimat, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium 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 8 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 Telekommunikationsdienste 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

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. 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 Anordnung nach § 60 Absatz 2 Satz 1, die
    a) der Gewährleistung flächendeckend angemessener und ausreichender Telekommunikationsdienstleistungen dient, oder
    b) einen anderen als unter Buchstabe a genannten Inhalt aufweist,

    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 zu Endkundenentgelten für regulierte intra-EU-Kommunikation sowie zur Änderung der Richtlinie 2002/22/EG und der Verordnung (EU) Nr. 531/2012 (ABl. L 310 vom 26.11.2015, S. 1), die zuletzt durch die Verordnung (EU) 2018/1971 (ABl. L 321 vom 17.12.2018, S. 1) geändert worden ist, 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,
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 oder
5. entgegen Artikel 5a Absatz 2 Satz 2 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet oder
6. entgegen Artikel 5a Absatz 5 Satz 1 als Anbieter regulierter intra-EU-Kommunikation eine dort genannte Obergrenze nicht oder nicht richtig festlegt.

(1c) Ordnungswidrig handelt, wer als Anbieter regulierter intra-EU-Kommunikation nach Artikel 2 Absatz 2 Nummer 3 der Verordnung (EU) 2015/2120 vorsätzlich oder fahrlässig
1. gegenüber einem Verbraucher einen Endkundenpreis berechnet, der den in Artikel 5a Absatz 1 der Verordnung (EU) 2015/2120 genannten Endkundenpreis überschreitet,
2. nicht sicherstellt, dass ein in Artikel 5a Absatz 3 der Verordnung (EU) 2015/2120 genannter Tarifwechsel durchgeführt wird oder
3. nicht sicherstellt, dass ein Verbraucher gemäß Artikel 5a Absatz 4 der Verordnung (EU) 2015/2120 aus einem oder in einen dort genannten Tarif kostenfrei wechseln kann.

(1d) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018 über Maßnahmen gegen ungerechtfertigtes Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts und zur Änderung der Verordnungen (EG) Nr. 2006/2004 und (EU) 2017/2394 sowie der Richtlinie 2009/22/EG (ABl. L 60 I vom 2.3.2018, S. 1) verstößt, indem er vorsätzlich oder fahrlässig
1. entgegen Artikel 3 Absatz 1 einen Zugang zur Online-Benutzeroberfläche sperrt oder beschränkt,
2. entgegen Artikel 3 Absatz 2 einen Kunden zu einer dort genannten Version der Online-Benutzeroberfläche weiterleitet,
3. entgegen Artikel 4 Absatz 1 unterschiedliche allgemeine Geschäftsbedingungen anwendet oder
4. entgegen Artikel 5 Absatz 1 unterschiedliche Bedingungen für einen Zahlungsvorgang anwendet.

(2) Die Ordnungswidrigkeit kann wie folgt geahndet werden:

1. in den Fällen des Absatzes 1 Nummer 12 Buchstabe a mit einer Geldbuße bis zu einer Million Euro, abweichend hiervon bei einer juristischen Person oder Personenvereinigung mit einem durchschnittlichen Jahresumsatz von mehr als 50 Millionen Euro mit einer Geldbuße bis zu 2 Prozent des durchschnittlichen Jahresumsatzes; bei der Ermittlung des durchschnittlichen Jahresumsatzes ist der weltweit erzielte Umsatz aller Unternehmen im Sinne des § 3 Nummer 29 der letzten drei Geschäftsjahre, die der Behördenentscheidung vorausgehen, zugrunde zu legen; der durchschnittliche Jahresumsatz kann geschätzt werden,
2. 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,
3. in den Fällen des Absatzes 1 Nummer 7a, 16 bis 17a, 18, 26, 29, 30a, 33, 41 bis 43 und des Absatzes 1d mit einer Geldbuße bis zu dreihunderttausend Euro,
4. 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, des Absatzes 1b Nummer 2 und 5 und des Absatzes 1c mit einer Geldbuße bis zu hunderttausend Euro,
5. 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
6. 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

Datenschutz-Grundverordnung (DSGVO)
– auszugsweise –

Der nachfolgende Text der Datenschutz-Grundverordnung entspricht der im Amtsblatt der Europäischen Union am 4. Mai 2016 unter L 119/1 veröffentlichten, im Amtsblatt der Europäischen Union am 22. November 2016 unter L 314/72 und am 23. Mai 2018 unter L127/2 berichtigten amtlichen Fassung.

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

Nichtamtliche Inhaltsübersicht

KAPITEL V
Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

KAPITEL VI
Unabhängige Aufsichtsbehörden

Abschnitt 2
Zuständigkeit, Aufgaben und Befugnisse

KAPITEL VIII
Rechtsbehelfe, Haftung und Sanktionen

KAPITEL XI
Schlussbestimmungen

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16, auf Vorschlag der Europäischen Kommission, nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente, nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[1], nach Stellungnahme des Ausschusses der Regionen[2], gemäß dem ordentlichen Gesetzgebungsverfahren[3], in Erwägung nachstehender Gründe.

(1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

(3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates[4] ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

(4) Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere

1 ABl. C 229 vom 31.7.2012, S. 90.
2 ABl. C 391 vom 18.12.2012, S. 127.
3 Standpunkt des Europäischen Parlaments vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 14. April 2016.
4 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. L 281 vom 23.11.1995, S. 31).

Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen.

KAPITEL I
Allgemeine Bestimmungen

Artikel 1
Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Artikel 2
Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,
b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,
c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,
d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

(3) Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 98 an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.

(4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.

Artikel 3
Räumlicher Anwendungsbereich

(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Artikel 4
Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „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, wirt-

schaftlichen, kulturellen oder sozialen Identität dieser natürlichen 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 oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder 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, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen 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 personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;
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 dem Recht der Mitgliedstaaten möglicherweise 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. „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
11. „Einwilligung“ der betroffenen Person 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;
12. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
13. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;
14. „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, wie Gesichtsbilder oder daktyloskopische Daten;
15 „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;

16. „Hauptniederlassung“
    a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;
    b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;
17. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;
18. „Unternehmen“ eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;
19. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;
20. „verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern;
21. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige Stelle;
22. „betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil
    a) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,

b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder

c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

23. „grenzüberschreitende Verarbeitung“ entweder

a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

24. „maßgeblicher und begründeter Einspruch“ einen Einspruch gegen einen Beschlussentwurf im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder ob beabsichtigte Maßnahmen gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;

25. „Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates[5];

26. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

5 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).

KAPITEL II
Grundsätze

Artikel 5
Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung");

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit");

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung");

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Artikel 6
Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder
b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese

Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Artikel 7
Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so 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. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(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 wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Artikel 8
Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

(1) Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.

Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

(2) Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewis-

sern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

(3) Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

Artikel 9
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,
c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,
d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,
f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,
g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,
h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, 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- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,
i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder
j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die eben-

falls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Artikel 10
Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

Artikel 11
Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

(1) Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

(2) Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

KAPITEL III
Rechte der betroffenen Person

Abschnitt 1
Transparenz und Modalitäten

Artikel 12
Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

(2) Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und

über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
b) sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(6) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

(7) Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.

Abschnitt 2
Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Artikel 13
Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:
a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Artikel 14
Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) die Kategorien personenbezogener Daten, die verarbeitet werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Lö-

schung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2
a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,
b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,
c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(4) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit
a) die betroffene Person bereits über die Informationen verfügt,
b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der

berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,

c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder

d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Artikel 15
Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;
b) die Kategorien personenbezogener Daten, die verarbeitet werden;
c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die

geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann die Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person einen Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Abschnitt 3
Berichtigung und Löschung

Artikel 16
Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Artikel 17
Recht auf Löschung („Recht auf Vergessenwerden“)

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist
a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Artikel 18
Recht auf Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:
a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

c) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

(3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

Artikel 19
Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Artikel 20
Recht auf Datenübertragbarkeit

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern
a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und
b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3) Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) Das Recht gemäß Absatz 1 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Abschnitt 4
Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

Artikel 21
Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

(3) Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

(4) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(5) Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

(6) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

Artikel 22
Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt

(2) Absatz 1 gilt nicht, wenn die Entscheidung
a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Abschnitt 5
Beschränkungen

Artikel 23
Beschränkungen

(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) die nationale Sicherheit;
b) die Landesverteidigung;
c) die öffentliche Sicherheit;
d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;
e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;
f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;
g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;
h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;
i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;
j) die Durchsetzung zivilrechtlicher Ansprüche.

(2) Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf

a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,
b) die Kategorien personenbezogener Daten,
c) den Umfang der vorgenommenen Beschränkungen,
d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung;

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,
f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,
g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und
h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

KAPITEL IV
Verantwortlicher und Auftragsverarbeiter

Abschnitt 1
Allgemeine Pflichten

Art. 24
Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

Art. 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) 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 trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Artikel 28
Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen

Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im

Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 93 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Abschnitt 2
Sicherheit personenbezogener Daten

Artikel 32
Sicherheit der Verarbeitung

(1) 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 des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Artikel 33
Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:
a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Artikel 34
Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;
c) 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 betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

Abschnitt 3
Datenschutz-Folgenabschätzung und vorherige Konsultation

Artikel 35
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 ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des

Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

KAPITEL V
Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

Artikel 44
Allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Artikel 45
Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art – auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten – sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbe-

helfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und bei internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 des vorliegenden Artikels erlassenen Beschlüsse und der nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen beeinträchtigen könnten.

(5) Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen – insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung – dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2

des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 93 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

(6) Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat.

(7) Übermittlungen personenbezogener Daten an das betreffende Drittland, das Gebiet oder einen oder mehrere spezifische Sektoren in diesem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 46 bis 49 werden durch einen Beschluss nach Absatz 5 des vorliegenden Artikels nicht berührt.

(8) Die Kommission veröffentlicht im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, für die sie durch Beschluss festgestellt hat, dass sie ein angemessenes Schutzniveau gewährleisten bzw. nicht mehr gewährleisten.

(9) Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie durch einen nach dem Prüfverfahren gemäß den Absätzen 3 oder 5 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 46
Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,
b) verbindlichen internen Datenschutzvorschriften gemäß Artikel 47,

c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,
d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 genehmigt wurden,
e) genehmigten Verhaltensregeln gemäß Artikel 40 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder
f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

(3) Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien gemäß Absatz 1 auch insbesondere bestehen in
a) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder
b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

(4) Die Aufsichtsbehörde wendet das Kohärenzverfahren nach Artikel 63 an, wenn ein Fall gemäß Absatz 3 des vorliegenden Artikels vorliegt.

(5) Von einem Mitgliedstaat oder einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilte Genehmigungen bleiben so lange gültig, bis sie erforderlichenfalls von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden. Von der Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie erforderlichenfalls mit einem nach Absatz 2 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 47
Verbindliche interne Datenschutzvorschriften

(1) Die zuständige Aufsichtsbehörde genehmigt gemäß dem Kohärenzverfahren nach Artikel 63 verbindliche interne Datenschutzvorschriften, sofern diese

a) rechtlich bindend sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern durchgesetzt werden, und dies auch für ihre Beschäftigten gilt,
b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen und
c) die in Absatz 2 festgelegten Anforderungen erfüllen.

(2) Die verbindlichen internen Datenschutzvorschriften nach Absatz 1 enthalten mindestens folgende Angaben:

a) Struktur und Kontaktdaten der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und jedes ihrer Mitglieder;
b) die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;
c) interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften;
d) die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundene Stellen;
e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung nach Artikel 22 unterworfen zu werden sowie des in Artikel 79 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;
f) die von dem in einem Mitgliedstaat niedergelassenen Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unterneh-

mensgruppe gegen die verbindlichen internen Datenschutzvorschriften; der Verantwortliche oder der Auftragsverarbeiter ist nur dann teilweise oder vollständig von dieser Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;

g) die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Artikel 13 und 14 hinaus über die verbindlichen internen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;

h) die Aufgaben jedes gemäß Artikel 37 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen internen Datenschutzvorschriften in der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;

i) die Beschwerdeverfahren;

j) die innerhalb der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens einer Unternehmensgruppe oder der Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden;

k) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;

l) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe j genannten Maßnahmen gegenüber der Aufsichtsbehörde;

m) die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen internen Datenschutzvorschriften bieten, und

n) geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.

(3) Die Kommission kann das Format und die Verfahren für den Informationsaustausch über verbindliche interne Datenschutzvorschriften im Sinne des vorliegenden Artikels zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

Artikel 48
Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung

Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Artikel 49
Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,
b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,
c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,
d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,
e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,

f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,
g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 – einschließlich der verbindlichen internen Datenschutzvorschriften – gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.

(2) Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

(3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und sowie Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.

(5) Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.

(6) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 Unterabsatz 2 des vorliegenden Artikels in der Dokumentation gemäß Artikel 30.

KAPITEL VI
Unabhängige Aufsichtsbehörden

Abschnitt 2
Zuständigkeit, Aufgaben und Befugnisse

Artikel 56
Zuständigkeit der federführenden Aufsichtsbehörde

(1) Unbeschadet des Artikels 55 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters gemäß dem Verfahren nach Artikel 60 die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung.

(2) Abweichend von Absatz 1 ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen diese Verordnung zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt.

(3) In den in Absatz 2 des vorliegenden Artikels genannten Fällen unterrichtet die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit. Innerhalb einer Frist von drei Wochen nach der Unterrichtung entscheidet die federführende Aufsichtsbehörde, ob sie sich mit dem Fall gemäß dem Verfahren nach Artikel 60 befasst oder nicht, wobei sie berücksichtigt, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat oder nicht.

(4) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall zu befassen, so findet das Verfahren nach Artikel 60 Anwendung. Die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, kann dieser einen

Beschlussentwurf vorlegen. Die federführende Aufsichtsbehörde trägt diesem Entwurf bei der Ausarbeitung des Beschlussentwurfs nach Artikel 60 Absatz 3 weitestgehend Rechnung.

(5) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall nicht selbst zu befassen, so befasst die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, sich mit dem Fall gemäß Artikeln 61 und 62.

(6) Die federführende Aufsichtsbehörde ist der einzige Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung.

Artikel 57
Aufgaben

(1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

a) die Anwendung dieser Verordnung überwachen und durchsetzen;
b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;
c) im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten;
d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren;
e) auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeiten;
f) sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;
g) mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;

h) Untersuchungen über die Anwendung dieser Verordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;
i) maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;
j) Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 und des Artikels 46 Absatz 2 Buchstabe d festlegen;
k) eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß Artikel 35 Absatz 4 eine Datenschutz-Folgenabschätzung durchzuführen ist;
l) Beratung in Bezug auf die in Artikel 36 Absatz 2 genannten Verarbeitungsvorgänge leisten;
m) die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Absatz 1 fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 bieten müssen, Stellungnahmen abgeben und sie billigen;
n) die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 billigen;
o) gegebenenfalls die nach Artikel 42 Absatz 7 erteilten Zertifizierungen regelmäßig überprüfen;
p) die Anforderungen an die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 abfassen und veröffentlichen;
q) die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 vornehmen;
r) Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 genehmigen;
s) verbindliche interne Vorschriften gemäß Artikel 47 genehmigen;
t) Beiträge zur Tätigkeit des Ausschusses leisten;
u) interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 ergriffene Maßnahmen und
v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

(2) Jede Aufsichtsbehörde erleichtert das Einreichen von in Absatz 1 Buchstabe f genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Die Erfüllung der Aufgaben jeder Aufsichtsbehörde ist für die betroffene Person und gegebenenfalls für den Datenschutzbeauftragten unentgeltlich.

(4) Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anfragen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

Artikel 58
Befugnisse

(1) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

a) den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,
b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,
c) eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen,
d) den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,
e) von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,
f) gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,
b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,
c) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,
d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen,
f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,
h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,
i) eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,
j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

(3) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Genehmigungsbefugnisse und beratenden Befugnisse, die es ihr gestatten,
a) gemäß dem Verfahren der vorherigen Konsultation nach Artikel 36 den Verantwortlichen zu beraten,
b) zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaats an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten,
c) die Verarbeitung gemäß Artikel 36 Absatz 5 zu genehmigen, falls im Recht des Mitgliedstaats eine derartige vorherige Genehmigung verlangt wird,
d) eine Stellungnahme abzugeben und Entwürfe von Verhaltensregeln gemäß Artikel 40 Absatz 5 zu billigen,
e) Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren,
f) im Einklang mit Artikel 42 Absatz 5 Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen,
g) Standarddatenschutzklauseln nach Artikel 28 Absatz 8 und Artikel 46 Absatz 2 Buchstabe d festzulegen,
h) Vertragsklauseln gemäß Artikel 46 Absatz 3 Buchstabe a zu genehmigen,
i) Verwaltungsvereinbarungen gemäß Artikel 46 Absatz 3 Buchstabe b zu genehmigen,
j) verbindliche interne Vorschriften gemäß Artikel 47 zu genehmigen.

(4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.

(5) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen dieser Verordnung durchzusetzen.

(6) Jeder Mitgliedstaat kann durch Rechtsvorschriften vorsehen, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 2 und 3 aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. Die Ausübung dieser Befugnisse darf nicht die effektive Durchführung des Kapitels VII beeinträchtigen.

KAPITEL VIII
Rechtsbehelfe, Haftung und Sanktionen

Artikel 82
Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

KAPITEL XI
Schlussbestimmungen

Artikel 95
Verhältnis zur Richtlinie 2002/58/EG

Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

Artikel 99
Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Geschehen zu Brüssel am 27. April 2016.

Anhang 3

Bundesdatenschutzgesetz (BDSG)
– auszugsweise –

vom 30. Juni 2017 (BGBl. I S. 2097),
das durch Artikel 12 des Gesetzes vom 20. November 2019
(BGBl. I S. 1626) geändert worden ist

Inhaltsübersicht

Teil 2
Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679

Kapitel 1
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Abschnitt 2
Besondere Verarbeitungssituationen

Kapitel 2
Rechte der betroffenen Person

Kapitel 4
Aufsichtsbehörde für die Datenverarbeitung durch nichtöffentliche Stellen

Teil 3
Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

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; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung 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 den Mitgliedstaaten der Europäischen Union gleich.[1] 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.

1 § 1 Abs. 6 Satz 1: IdF d. Art. 12 Nr. 2 Buchst. b G v. 20.11.2019/1626 mWv 26.11.2019.

§ 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 4
Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

§ 9
Zuständigkeit

(1) Die oder der Bundesbeauftragte[2] ist zuständig für die Aufsicht über die öffentlichen Stellen des Bundes, auch soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, sowie über Unternehmen, soweit diese für die geschäftsmäßige Erbringung von Telekommunikationsdienstleistungen Daten von natürlichenoder juristischen Personen verarbeiten und sich die Zuständigkeit nicht bereits aus § 115 Absatz 4 des Telekommunikationsgesetzes ergibt. 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.

Teil 2
Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verorndung (EU) 2016/679

Kapitel 1
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Abschnitt 2
Besondere Verarbeitungssituationen

§ 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

2 § 9 Abs. 1 Satz 1: IdF d. Art. 12 Nr. 4 G v. 20.11.2019/1626 mWv 26.11.2019.

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[3]

(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)[4] 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

3 § 32: zur Anwendung vgl. § 4 Abs. 4.
4 § 32 Abs. 2: zur Anwendung vgl. § 85 Abs. 3.

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 Ansprüche beeinträchtigen würde oder die Verarbeitung Daten aus zivilrechtlichen 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 festgestellt 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)[5] 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;

5 § 33 Abs. 2: zur Anwendung vgl. § 85 Abs. 3.

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.

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.[6] 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.

6 § 40 Abs. 3 Satz 1: zur Anwendung vgl. § 16 Abs. 5.

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.

Teil 3
Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 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.

Anhang 4

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,[1]

nach Stellungnahme des Wirtschafts- und Sozialausschusses,[2]

nach Anhörung des Ausschusses der Regionen,

gemäß dem Verfahren des Artikels 251 des Vertrags,[3]

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 sicher-

1 ABl. C 365 E vom 19.12.2000, S. 223.
2 ABl. C 123 vom 25.4.2001, S. 53.
3 Stellungnahme des Europäischen Parlaments vom 13. November 2001 (noch nicht im Amtsblatt veröffentlicht), Gemeinsamer Standpunkt des Rates vom 28. Januar 2002 (ABl. C 113 E vom14.5.2002, S. 39) und Beschluss des Europäischen Parlaments vom 30. Mai 2002 (noch nicht im Amtsblatt veröffentlicht). Beschluss des Rates vom 25. Juni 2002.
4 ABl. L 281 vom 23.11.1995, S. 31.

stellen, 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 Richtlinie 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

5 ABl. L 24 vom 30.1.1998, S. 1.

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 Endgerät 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 kön-

nen 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 Teilnehmer 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 Ein-

satz 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 Verarbeitung 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 sollten 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

6 ABl. L 178 vom 17.7.2000, S. 1.
7 ABl. L 91 vom 7.4.1999, S. 10.

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.

8 ABl. L 108 vom 24.4.2002, S. 33.

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.

9 ABl. L 204 vom 21.7.1998, S. 37. Richtlinie geändert durch die Richtlinie 98/48/EG (ABl. L 217 vom 5.8.1998, S. 18).
10 ABl. L 36 vom 7.2.1987. Beschluss zuletzt geändert durch die Beitrittsakte von 1994.

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 ver-

bleiben, 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 5

Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz – UrhG) – auszugsweise –

vom 9. September 1965 (BGBl. I S. 1273),
das zuletzt durch Artikel 1 des Gesetzes vom 28. November 2018
(BGBl. I S. 2014) geändert worden ist

Inhaltsübersicht

Teil 4
Gemeinsame Bestimmungen für Urheberrecht und verwandte Schutzrechte

Abschnitt 2
Rechtsverletzungen

Unterabschnitt 1
Bürgerlich-rechtliche Vorschriften; Rechtsweg

§ 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 6

Strafprozessordnung (StPO)
– auszugsweise –

in der Fassung der Bekanntmachung vom 7. April 1987
(BGBl. I S. 1074, 1319),
die zuletzt durch Artikel 3 des Gesetzes vom 10. Juli 2020
(BGBl. I S. 1648) geändert worden ist

Inhaltsübersicht

Erstes Buch
Allgemeine Vorschriften

Achter Abschnitt
Ermittlungsmaßnahmen

Erstes Buch
Allgemeine Vorschriften

Achter Abschnitt
Ermittlungsmaßnahmen

§ 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, Wohnungseinbruchdiebstahl nach § 244 Absatz 4 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) Vorenthalten und Veruntreuen von Arbeitsentgelt unter den in § 266a Absatz 4 Satz 2 Nummer 4 genannten Voraussetzungen,
r) 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,
s) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,
t) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,
u) 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,
v) 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 entge-

gennehmen 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 Über-

prüfung 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 und § 2a Absatz 1 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) 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 gespeicherter (retrograder) Standortdaten ist nach diesem Absatz nur unter den Voraussetzungen des Absatzes 2 zulässig. Im Übrigen ist die Erhebung von Standortdaten 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 ange-

messenen 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 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 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 er-

langte 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 entsprechend, 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 von Telekommunikationsdiensten, 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 7

Strafgesetzbuch (StGB)
– auszugsweise –

in der Fassung der Bekanntmachung vom 13. November 1998
(BGBl. I S. 3322),
das zuletzt durch Artikel 5 des Gesetzes vom 10. Juli 2020
(BGBl. I S. 1648) geändert worden ist

Inhaltsübersicht

Besonderer Teil

Besonderer Teil

Fünfzehnter Abschnitt
Verletzung des persönlichen Lebens- und Geheimbereichs

§ 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 8

Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV)

in der Fassung der Bekanntmachung vom 11. Juli 2017
(BGBl. I S. 2316),
die zuletzt durch Artikel 27 des Gesetzes vom 20. November 2019
(BGBl. I S. 1724) geändert worden ist

Nichtamtliches Inhaltsverzeichnis

Abschnitt 2
Technische Anforderungen

Abschnitt 3
Organisatorische Anforderungen, Schutzanforderungen

Abschnitt 4
Verfahren zum Nachweis nach § 110 Absatz 1 Satz 1 Nummer 3 des Telekommunikationsgesetzes

Abschnitt 5
Abweichungen

Teil 1
Allgemeine Vorschriften

§ 1
Gegenstand der Verordnung

Diese Verordnung regelt

1. die grundlegenden Anforderungen an die Gestaltung der technischen Einrichtungen, die für die Umsetzung der
   a) in § 100a Absatz 1 Satz 1 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 § 51 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.

§ 2
Begriffsbestimmungen

Im Sinne dieser Verordnung ist

1. Anordnung
   a) im Sinne der Teile 2 und 3 die Anordnung zur Überwachung der Telekommunikation nach § 100e der Strafprozessordnung, § 10 des Artikel 10-Gesetzes, § 23b des Zollfahndungsdienstgesetzes, § 51 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, § 52 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 § 100a Absatz 4 Satz 1 der Strafprozessordnung, § 1 Absatz 1 Nummer 1 des Artikel 10-Gesetzes, § 23a Absatz 1 Satz 1 des Zollfahndungsdienstgesetzes, § 51 Absatz 6 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 § 100a Absatz 4 Satz 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, § 52 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 § 100a Absatz 1 Satz 1 der Strafprozessordnung, den §§ 3, 5 oder 8 des Artikel 10-Gesetzes, den §§ 23a bis 23c des Zollfahndungsdienstgesetzes, § 51 Absatz 1 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 § 100a Absatz 1 Satz 1 der Strafprozessordnung, § 3 des Artikel 10-Gesetzes, den §§ 23a bis 23c und 23e des Zollfahndungsdienstgesetzes, § 51 Absatz 1 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. 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) § 100a Absatz 4 Satz 1 der Strafprozessordnung, § 2 Absatz 1 Satz 3 des Artikel 10-Gesetzes, § 23a Absatz 8 des Zollfahndungsdienstgesetzes, § 51 Absatz 6 Satz 1 des Bundeskriminalamtgesetzes 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 § 100a Absatz 1 Satz 1 der Strafprozessordnung, dem § 3 des

Artikel 10-Gesetzes, den §§ 23a bis 23c des Zollfahndungsdienstgesetzes, § 51 Absatz 1 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. 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 proto-

kollierten 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 An-

gaben 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 einge-

gangenen 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 Auswertungseinrichtungen 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 Schutzrechtsver-

merke 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. 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 Telekommunikations-

anschlüsse 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. 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 10 Gesetzes 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 Aufzeich-

nungs- 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. § 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 (§ 100a Absatz 4 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. I S. 458), zuletzt geändert durch Artikel 3 Absatz 18 des Gesetzes vom 7. Juli 2005 (BGBl. I S. 1970), oder das Einvernehmen nach § 16 der Fernmeldeverkehr-Überwachungs-Verordnung vom 18. Mai 1995 (BGBl. I S. 722), geändert durch Artikel 4 des Gesetzes vom 26. Juni 2001 (BGBl. I 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 9

Urteile des BVerfG und des EuGH zur Vorratsdatenspeicherung – auszugsweise –

BVerfG, Urteil des Ersten Senats vom 2. März 2010
– 1 BvR 256/08 –

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.

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.

EuGH, Urteil vom 8. April 2014
– C-293/12 –

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.

EuGH, Urteil vom 21. Dezember 2016
– C-203/15 und C-698/15 –

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 10

Anschriften der unabhängigen Datenschutzbehörden des Bundes und der Länder

Stand: August 2020

Bund	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	Prof. Ulrich Kelber Postfach 14 68 53004 Bonn	Tel.: 0228/997799-0 Fax: 0228/997799-5550 E-Mail: poststelle@bfdi.bund.de Internet: www.bfdi.bund.de
Baden-Württemberg	Landesbeauftragter 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			
Datenschutzbeauftragter des Landes	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
Aufsichtsbehörde für den nichtöffentlichen Bereich	Bayerisches Landesamt für Datenschutzaufsicht	Michael Will Postfach 13 49 91504 Ansbach Promenade 18 91522 Ansbach	Tel.: 0981/180093-0 Fax: 0981/180093-800 E-Mail: poststelle@lda.bayern.de Internet: www.lda.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 Brandenburg	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.: 0471/596 2010 oder 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 Ludwig-Erhard-Str. 22 20459 Hamburg	Tel.: 040/42854-4040 Fax: 040/42854-4000 E-Mail: mailbox@datenschutz.hamburg.de Internet: www.datenschutz-hamburg.de
Hessen	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit	Prof. Dr. Michael Ronellenfitsch Postfach 31 63 65021 Wiesbaden Gustav-Stresemann-Ring 1 65189 Wiesbaden	Tel.: 0611/1408-0 Fax: 0611/1408-900/901 E-Mail: poststelle@datenschutz.hessen.de Internet: www.datenschutz.hessen.de
Mecklenburg-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern	Heinz Müller Postanschrift: Schloss Schwerin Lennéstr. 1 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 Landesbeauftragte 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 Landesbeauftragte 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: 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	Sächsischer Datenschutzbeauftragter	Andreas Schurig Postfach 11 01 32 01330 Dresden Devrientstr. 5 01067 Dresden	Tel.: 0351/85471 101 Fax: 0351/85471 109 E-Mail: saechsdsb@slt.sachsen.de Internet: www.saechsdsb.de www.datenschutz.sachsen.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.sachsen-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

www.bfdi.bund.de