Der
Bundesbeauftragte
für den Datenschutz

BfD-Info 5

Datenschutz in der Telekommunikation

Impressum

Herausgeber:
Der Bundesbeauftragte für den Datenschutz
Postfach 20 01 12, 53131 Bonn
Hausanschrift: Husarenstraße 30, 53117 Bonn
Tel: (0228) 81995-0, Telefax: (0228) 81995-550
E-Mail: poststelle@bfd.bund.de
Internet: http://www.datenschutz.bund.de

Druck:
Präzis-Druck GmbH
Hedwigstraße 2-8
76199 Karlsruhe

Auflage: 6. Auflage, Februar 2004

Inhaltsverzeichnis

Das Telekommunikationsgesetz und die Telekommunikations-Datenschutzverordnung

Anhang 1: Gesetzes- und Verordnungstexte

Abkürzungsverzeichnis

ABl EG	Amtsblatt der Europäischen Gemeinschaft
AWG	Außenwirtschaftsgesetz
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BGBl.	Bundesgesetzblatt
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
CD-ROM	Compact Disc-Read Only Memory
DAV	Dienstanschlussvorschriften
DECT	Digital Enhanced Cordless Telecommunications
E-Mail	Electronic Mail = Elektronische Post
EVN	Einzelverbindungsnachweis
GG	Grundgesetz
G 10-G	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GSM	Global System for Mobile Communication
ISDN	Integrated Services Digital Network
IT	Informationstechnik
IuKDG	Informations- und Kommunikationsdienstegesetz
LfD	Landesbeauftragter für den Datenschutz
PC	Personal Computer
PIN	Personal Identification Number
PGP	Pretty Good Privacy
PtRegG	Postregulierungsgesetz
RegTP	Regulierungsbehörde für Telekommunikation und Post
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SMS	Short Message Service (Kurzmitteilung)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TKV	Telekommunikations-Kundenschutzverordnung
TUDLV	Telekommunikations-Universaldienstleistungsverordnung
WAP	Wireless Access Protocol

Vorwort

Datenschutz ist Grundrechtsschutz und damit wesentlicher Bestandteil einer freiheitlichen Gesellschaftsordnung. Dies gilt auch für den Bereich der Telekommunikation und das Internet. Die neuen Medien, die die Informations- und Wissensgesellschaft prägen, durchdringen sämtliche Lebensbereiche. Sie bestimmen damit wesentlich die Handlungs- und Kommunikationsfähigkeit der Bürgerinnen und Bürger. Die Stichworte, die diese Entwicklung veranschaulichen, heißen Digitalisierung, Medienkonvergenz und weltweite Vernetzung. Durch die weiter voranschreitende Miniaturisierung hält die elektronische Datenverarbeitung auch in ganz unscheinbare Dinge des alltäglichen Gebrauchs Einzug mit der Konsequenz, die Nutzung dieser Gegenstände zu registrieren und nachvollziehbar zu machen. Der technologische Fortschritt darf aber nicht dazu führen, dass die Freiheitsrechte der Menschen aus dem Blick geraten. Deshalb müssen auch diese dynamischen Entwicklungen aufmerksam begleitet werden, um Fehlentwicklungen zu vermeiden.

Auf bestimmte, mit den neuen Technologien für das Persönlichkeitsrecht des einzelnen Nutzers verbundene Risiken haben Bundestag und Bundesregierung mit so genannten bereichsspezifischen Datenschutzregelungen reagiert. So enthält das Telekommunikationsgesetz grundlegende Vorschriften zur Wahrung des Datenschutzes und des Fernmeldegeheimnisses, die den Schutz des informationellen Selbstbestimmungsrechts des Bürgers zum Ziel haben. Dadurch ist dem Datenschutz im Bereich der Telekommunikation in Deutschland ein sehr hoher Stellenwert zugewiesen.

Diese Broschüre soll die Bürgerinnen und Bürger über die verschiedenen datenschutzrechtlichen Regelungen im Bereich der Telekommunikation informieren und dazu beitragen, dass sie ihr Recht auf informationelle Selbstbestimmung wahren können.

Peter Schaar
Der Bundesbeauftragte für den Datenschutz

1 Zweck und Inhalt dieser Broschüre; Aktualisierungsbedarf

Diese Broschüre soll jedem interessierten Bürger einen Überblick über seine Datenschutzrechte im Zusammenhang mit der Nutzung von Telekommunikationsdiensten ermöglichen. In den einzelnen Kapiteln wird auf die einschlägigen Rechtsvorschriften Bezug genommen. Die wichtigsten Bestimmungen sind im Anhang 1 abgedruckt. Ergänzende Textdokumente, auf die in den einzelnen Kapiteln verwiesen wird, können in den Anhängen 2ff. nachgelesen werden.

Neben allgemeinen Sachinformationen werden auch Fragen behandelt, die in der Vergangenheit häufiger Gegenstand datenschutzrechtlicher Anfragen sowohl von Seiten der Bürger als auch von Seiten der Telekommunikationsdiensteanbieter gewesen sind.

Die Broschüre soll zugleich als Basisinformation für diejenigen dienen, die beruflich im Bereich der Telekommunikation mit personenbezogenen Daten umgehen.

Die Bundesregierung hat am 18. Dezember 2000 auf der Grundlage von § 89 Abs. 1 TKG die neue Telekommunikations-Datenschutzverordnung, die der Zustimmung des Bundesrates bedurfte, erlassen. Der hierdurch entstandene Aktualisierungsbedarf gab Veranlassung, die bisherige Broschüre vollständig zu überarbeiten und gleichzeitig die eingetretenen technischen und organisatorischen Weiterentwicklungen des liberalisierten Telekommunikationsmarktes zu berücksichtigen. Die vorliegende Neuauflage versucht, die komplexen technischen und rechtlichen Zusammenhänge im Bereich der modernen Telekommunikation nach den wesentlichen Sachgesichtspunkten bürgernah darzustellen.

Noch ein Hinweis: Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

2 Überblick über die bereichsspezifischen Regelungen zum Datenschutz in der Telekommunikation

Im folgenden wird ein kurzer Überblick zu den für den Telekommunikationsbereich einschlägigen bereichsspezifischen Gesetzen und Verordnungen mit datenschutzrechtlichen Inhalten gegeben.

2.1 Grundgesetz

Das in Art. 10 GG verfassungsrechtlich verankerte Fernmeldegeheimnis schützt den Einzelnen davor, dass der Inhalt sowie die näheren Umstände seiner Telekommunikation staatlichen Stellen zur Kenntnis gelangen (siehe Anhang 1 I.1). Beschränkungen dieses Grundrechts dürfen nur aufgrund eines Gesetzes angeordnet werden. Dabei bezeichnet der Begriff „Inhalt“ die mittels Telekommunikationsanlagen übermittelten individuellen Nachrichten, während mit den „näheren Umständen“ insbesondere die Verbindungsdaten eines Kommunikationsvorganges gemeint sind. Zu den näheren Umständen der Telekommunikation gehören:

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

Das verfassungsrechtlich geschützte Fernmeldegeheimnis besitzt jedoch keine unmittelbare Wirkung für den privaten Rechtsverkehr, also z.B. für das Verhältnis zwischen Telekommunikationsdiensteanbietern und ihren Kunden oder zwischen Bürgern untereinander. Art. 10 Grundgesetz regelt den Schutz des Fernmeldegeheimnisses vielmehr nur im Verhältnis zwischen Bürger und Staat.

2.2 Telekommunikationsgesetz

Im Rahmen der sog. Postreform hat der Bundesgesetzgeber vielfältige legislative Maßnahmen zur Privatisierung und Liberalisierung des Telekommunikationsmarktes in der Bundesrepublik Deutschland getroffen.

Insbesondere wurde die Wahrung des Fernmeldegeheimnisses daher durch die Vorschrift des § 85 TKG auch denjenigen aufgegeben, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken. Da das Fernmeldegeheimnis unabhängig davon sichergestellt werden muss, ob derartige Dienste mit oder ohne Gewinnerzielungsabsicht bzw. nur an bestimmte Personen oder der Öffentlichkeit gegenüber angeboten werden, sind im Rahmen des Telekommunikationsgesetzes auch die geschlossenen Benutzergruppen auf die Achtung des Fernmeldegeheimnisses verpflichtet worden.

Nicht vom Fernmeldegeheimnis erfasst werden dagegen in der Regel private Endgeräte, Haustelefonanlagen und hauseigene Sprechanlagen. Hier greifen lediglich die Strafvorschriften des Strafgesetzbuches gegen die Verletzung der Vertraulichkeit des gesprochenen Wortes ein.

Die bereichsspezifischen datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes (siehe Anhang 1 II.1) sind im Elften Teil des Telekommunikationsgesetzes (§§ 85 - 93 TKG) geregelt. Von besonderer datenschutzrechtlicher Relevanz ist die Vorschrift des § 89 TKG. Dort werden die datenschutzrechtlichen Grundsätze für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, festgelegt.

Gemäß § 89 Abs. 1 TKG hat die Bundesregierung mit Zustimmung des Bundesrates im Dezember 2000 die Telekommunikations-Datenschutzverordnung (siehe Anhang 1 II.3) als Rechtsverordnung zum Schutz personenbezogener Daten der an der Telekommunikation Beteiligten erlassen.

2.3 Telekommunikations-Datenschutzverordnung

Die Telekommunikations-Datenschutzverordnung (TDSV) ist am 21.12.2000 in Kraft getreten (siehe Anhang 1 II.3). Damit konnte nach fünf Jahren ein Rechtssetzungsvorhaben abgeschlossen werden, das zugunsten der Nutzer von Telekommunikationsdiensten Rechtsicherheit schafft.

Vorläufer der TDSV war die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV 1996) vom 12. Juli 1996. Die TDSV 1996 wurde seinerzeit von der Bundesregierung aufgrund von § 10 Abs. 1 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) beschlossen. Aufgrund von unterschiedlichen Regelungen zwischen § 10 PTRegG und deren Nachfolgevorschrift, nämlich § 89 TKG, war es schon kurze Zeit später zu Wertungswidersprüchen gekommen. Nach § 10 Abs. 1 PTRegG und damit auch nach § 1 Abs. 1 TDSV 1996 mussten die bereichsspezifischen Datenschutzregelungen im Bereich der Telekommunikation nur von den Unternehmen beachtet werden, die ihre Leistungen der Öffentlichkeit, d.h. gegenüber jedermann anboten. Demgegenüber erweiterte § 89 Abs. 1 TKG den Adressatenkreis um die sogenannten geschäftsmäßigen Anbieter von Telekommunikationsdiensten. Darunter versteht man Dienste, die ihre Leistungen nicht jedermann, sondern nur bestimmten Dritten zur Verfügung stellen, wobei es unerheblich ist, ob dies mit oder ohne Gewinnerzielungsabsicht erfolgt. Ohne Bedeutung ist in diesem Zusammenhang auch die Anzahl der berechtigten Nutzer derartiger Telekommunikationsdienste. Hintergrund für die Erweiterung der verpflichteten Normadressaten war die Überlegung, dass die Nutzer von Telekommunikationsdiensten ihr Recht auf informationelle Selbstbestimmung, das im Bereich der Telekommunikation noch durch den ihnen zustehenden Anspruch auf Wahrung des Fernmeldegeheimnisses ergänzt wird, unabhängig von der Frage geschützt wissen wollen, ob die dabei anfallenden personenbezogenen Daten durch eine Telefongesellschaft oder beispielsweise im Rahmen eines konzernweiten Corporate Networks verarbeitet und genutzt werden. Vor diesem Hintergrund sollten z.B. auch die Betreiber von Nebenstellenanlagen in Betrieben und Behörden die bereichsspezifischen Datenschutzregelungen von § 89 TKG bzw. der entsprechenden Rechtsverordnung beachten, soweit die Beschäftigten, die dort vorgehaltenen Telekommunikationsanlagen auch zu privaten Zwecken nutzen dürfen.

Neben der grundsätzlichen Frage des Anwendungsbereiches der fraglichen Normen galt es, bei der Novellierung der TDSV 1996 weitere unterschiedliche Regelungen zwischen Gesetz und Verordnung zu harmonisieren. So ist nach § 89 TKG in bestimmten Fällen die Datenverarbeitung und -nutzung nur zulässig, wenn der Betroffene zuvor eingewilligt hat. Dies musste in die entsprechenden Bestimmungen der Rechtsverordnung übernommen werden. Zudem war es erforderlich, begriffliche Definitionen anzugleichen und zu vereinheitlichen.

2.4 Telekommunikations-Kundenschutzverordnung

Die Telekommunikations-Kundenschutzverordnung (TKV), die von der Bundesregierung mit Zustimmung des Bundesrates nach § 41 TKG erlassen wurde, schafft einen Rahmen zur Regelung der Vertragsverhältnisse zwischen den Anbietern von Telekommunikationsdienstleistungen für die Öffentlichkeit und ihren Kunden. Sie dient dem Schutz der Verbraucher (siehe Anhang 1 II.5). Daneben enthält die Verordnung weitere Regelungen, die nur marktbeherrschende Unternehmen verpflichten. Sie sollen den Kunden vor missbräuchlicher Ausnutzung der Marktmacht durch diese Unternehmen schützen.

Datenschutzrechtlichen Bezug haben nur vereinzelte Regelungen der TKV. In der Praxis besonders wichtig ist z.B. die Regelung zur Erstellung von Einzelverbindungsnachweisen in § 14 TKV (siehe 4.5.4.1). Danach haben die Telekommunikationsdiensteanbieter ihren Kunden die Standardform eines Einzelverbindungsnachweises unentgeltlich zur Verfügung zu stellen.

Für den Kunden ist auch die Vorschrift für die Rechnungserstellung in § 15 TKV relevant. Danach hat jeder das Recht, von dem Telekommunikationsunternehmen, bei dem er seinen Zugang zum öffentlichen Telekommunikationsnetz hat, eine Gesamtrechnung für alle Verbindungen zu erhalten, die von diesem Anschluss ausgegangen sind. Zumindest die Gesamthöhe der auf die einzelnen Anbieter entfallenen Entgelte müssen auf der Rechnung erkennbar sein. Bei Einwendungen gegen die Höhe einer Rechnung kann gemäß § 16 Abs. 1 TKV auch ohne Antrag des Kunden eine Auflistung der einzelnen Verbindungen erstellt werden. Dabei ist aber der Schutz von Mitbenutzern zu wahren.

Für den Eintrag in öffentliche Teilnehmerverzeichnisse (siehe 4.5.2.1) legt § 21 TKV den Anspruch fest, unentgeltlich eingetragen zu werden.

Bei Fragen zum Verbraucherschutz nach der TKV können Sie sich an den Verbraucherservice der Regulierungsbehörde für Telekommunikation und Post wenden. Dieser ist telefonisch zu erreichen unter:

01805/10 10 00 oder 030/2 24 80-500

Die Postanschrift lautet:

Regulierungsbehörde für Telekommunikation
und Post

Verbraucherservice
Postfach 80 01
53105 Bonn

2.5 EG- Datenschutzrichtlinie für elektronische Kommunikation

Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation - kurz EG-Datenschutzrichtlinie für elektronische Kommunikation genannt - betrifft die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft (siehe Anhang 1 II 4). Regelungsgegenstände sind u.a. die Netzsicherheit und die Vertraulichkeit der Kommunikation, die Datenverarbeitung für die Entgeltberechnung, die Nutzung von Standortdaten, die Rufnummernanzeige, die automatische Anrufweiterschaltung, die Gestaltung von Teilnehmerverzeichnissen, die Zulässigkeit unerbetener Werbung sowie Einzelheiten zu technischen Merkmalen und Normungen. In den Erwägungsgründen wird als Ziel auch die Möglichkeit der anonymen Nutzung von Kommunikationsdiensten genannt und damit eine Forderung des Bundesbeauftragten für den Datenschutz aufgegriffen.

Die zuvor bestehende EG-Telekommunikations-Datenschutzrichtlinie 97/66/EG vom 15.12.1997 wurde mit Wirkung vom 31.10.2003 aufgehoben.

In der neuen Richtlinie wurden die bisherigen Bestimmungen an neue und vorhersehbare Entwicklungen auf dem Gebiet elektronischer Kommunikationsdienste und -technologien angepasst. Der Anwendungsbereich der Richtlinie umfasst jetzt nicht mehr nur die Telekommunikationsdienste, sondern wurde auf alle elektronischen Kommunikationsnetze und -dienste ausgedehnt.
Neu aufgenommen wurde z.B. eine Regelung über die Verarbeitung sog. Standortdaten. Damit soll eine Schutzvorschrift zugunsten der Nutzer von Mobilfunkgeräten und Telematikdiensten geschaffen werden. Damit der Bürger in Zukunft nicht nur vor unerbetenen Anrufen, sondern auch gegen unerwünschte E-Mails geschützt ist, wurde der Anwendungsbereich der entsprechenden Vorschrift erweitert.

Die Richtlinie betrifft gemäß Art. 3 Abs. 1 unmittelbar zwar nur allgemein zugängliche Kommunikationsdienste in öffentlichen Kommunikationsnetzen. Der interne Kommunikationsverkehr in geschlossenen Benutzergruppen ist durch die Richtlinie

daher nicht berührt. Sobald jedoch eine Verbindung zwischen einem Teilnehmer eines solchen Corporate Networks und einem Teilnehmer eines öffentlichen Kommunikationsnetzes hergestellt ist, sind die Regelungen der Richtlinie dennoch zu beachten. Zudem sind die Mitgliedstaaten nicht gehindert, entsprechende Regelungen für den Kreis der geschlossenen Benutzergruppen in dem jeweiligen nationalen Datenschutzrecht zu schaffen, wie es in Deutschland der Fall ist.

Unmittelbare Rechtswirkungen gegenüber dem Bürger ergeben sich aus einer EU-Richtlinie nicht. Sie verpflichtet vielmehr die Gesetzgeber der Mitgliedstaaten zur Schaffung nationaler Rechtsvorschriften. Mittelbare Wirkung für den Bürger haben sie allerdings insoweit, als sie Maßstab für die Auslegung bestehender Vorschriften sind.

Die Richtlinie sollte bis zum 31. Oktober 2003 in nationales Recht umgesetzt werden. Diese Frist wurde nicht eingehalten. Eine Umsetzung erfolgt für den Datenschutz in der Telekommunikation durch eine Novellierung des Telekommunikationsgesetzes, die bei Redaktionsschluss noch nicht abgeschlossen war. Eine Regelung für den Schutz des Bürgers vor unerbetener Direktwerbung soll noch im Rahmen einer Änderung des Gesetzes gegen den unlauteren Wettbewerb getroffen werden.

2.6 Informations- und Kommunikationsdienste - Gesetz

Mit dem Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste - kurz Informations- und Kommunikationsdienste-Gesetz (IuKDG) genannt - wurden im Jahre 1997 das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG) verabschiedet. Eine Novellierung beider Gesetze erfolgte Ende 2001 (siehe Anhang 1 III.1 u. 2).

Das TDG und das TDDSG treffen datenschutzrechtliche Regelungen im Zusammenhang mit der Nutzung von Telediensten; geregelt wird also nicht die Telekommunikation. Die Teledienste setzen allerdings, wie § 2 Abs. 1 TDG ausdrücklich feststellt, die Übermittlung von Inhalten mittels Telekommunikation voraus.

Demnach kann es sich – je nach den angebotenen Leistungen - bei den sogenannten Internet-Serviceprovidern um Anbieter von Telediensten oder um Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen, handeln. Dies hat zur Folge, dass diese Unternehmen auch Normadressaten von telekommunikationsspezifischen Datenschutzregelungen sind. Dies gilt für die

Anbieter von E-Mail- und SMS-Diensten, die Betreiber von Mailbox-Systemen sowie die Anbieter von Internettelefonie.

2.6.1 Teledienstegesetz

Das TDG gibt Anhaltspunkte für die Abgrenzung zwischen Telediensten und Telekommunikationsdienstleistungen (§ 2 TDG), stellt die Zulassungs- und Anmeldefreiheit von Telediensten fest, regelt die Anbieterkennzeichnung und - vor allem - die Verantwortlichkeit für den Inhalt von Telediensten (siehe Anhang 1 III.1).

2.6.2 Teledienstedatenschutzgesetz

Das TDDSG ist die bereichsspezifische Datenschutzregelung für die Nutzung von Telediensten. Auch hier gilt das Verbot mit Erlaubnisvorbehalt (siehe 3.2). Das Gesetz enthält klare Regelungen zur Zweckbindung, zur Einwilligung des Nutzers in die Datenverarbeitung (die auch elektronisch erfolgen kann), zu Unterrichtungspflichten, zu den technischen und organisatorischen Voraussetzungen für den Datenschutz, zur Behandlung von Bestandsdaten, von Nutzungs- und Abrechnungsdaten, zu Auskunftsrechten des Nutzers sowie zur Datenschutzkontrolle (siehe Anhang 1 III.2).

In das TDDSG wurden erstmals konkrete Regelungen über die elektronische Einwilligung (§ 4 Abs. 2) aufgenommen.

Neu ist ferner, dass dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen ist, soweit dies technisch möglich und zumutbar ist (§ 4 Abs. 6).

Die Zuständigkeit für Datenschutzkontrollen im Zusammenhang mit der Nutzung von Telediensten liegt bei den Aufsichtsbehörden der Länder (Anschriften siehe Anhang 11). Der Bundesbeauftragte für den Datenschutz hat gemäß § 8 TDDSG - soweit es das Angebot und die Nutzung von Telediensten angeht - lediglich eine beobachtende Funktion.

Die Zuständigkeit für die datenschutzrechtliche Behandlung konkreter Einzelfragen - insbesondere von Nutzern von Telediensten - ist abhängig von dem konkret zu beurteilenden Sachverhalt, also vom Inhalt der Kundenbeschwerde oder des Beratungswunsches. Die Erfahrung hat gezeigt, dass die Mehrzahl der

datenschutzrechtlichen Probleme bei den Internet-Serviceprovidern nicht den Telekommunikationsdienst, sondern den jeweiligen Teledienst betreffen.

Angesichts der unterschiedlichen Kontrollzuständigkeiten ist eine Abstimmung und Zusammenarbeit der beteiligten Stellen, wie sie § 26 Abs. 4 BDSG vorsieht, erforderlich.

Sofort nach Inkrafttreten des Gesetzes begann die Evaluierung, die durch einen Bericht des Bundesministeriums für Wirtschaft und Technologie im Juni 1999 abgeschlossen wurde. Als Ergebnis des Berichts wurde Ende 2001 das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr erlassen. In diesem Rahmen wurden sowohl das Teledienstegesetz als auch das Teledienstedatenschutzgesetz novelliert.

Jeder Nutzer von Telediensten sollte darauf achten, dass die Anbieter deutliche Hinweise zum Datenschutz machen (privacy policy) und über den Umfang und Zweck der Datenerhebung, -verarbeitung und -nutzung unterrichten.

2.7 Telekommunikations-Überwachungsverordnung

Das Abhören und/oder Aufzeichnen von Telekommunikationsinhalten sowie die Erfassung der näheren Umstände ist nur im Auftrag staatlicher Stellen zulässig. § 88 Abs. 2 TKG ermächtigt die Bundesregierung, eine Verordnung zu erlassen, die die technischen und organisatorischen Vorgaben für die Betreiber von Telekommunikationsanlagen zur Umsetzung von Überwachungsmaßnahmen regelt. Die Telekommunikations-Überwachungsverordnung ist Anfang 2002 in Kraft getreten (siehe Anhang 1 II.2).

Die materiellen Voraussetzungen für die Telekommunikationsüberwachung regeln die einschlägigen Vorschriften der Strafprozessordnung, des G-10-Gesetzes sowie des Außenwirtschaftsgesetzes und nicht die TKÜV. Nach diesen Vorschriften trifft die Verpflichtung, Überwachungsmaßnahmen im Bereich der Telekommunikation zu ermöglichen, grundsätzlich nicht nur die Anbieter öffentlicher Telefonnetze, sondern jeden Betreiber einer Telekommunikationsanlage, der anderen den Netzzugang zu seiner Anlage geschäftsmäßig überlässt (§ 88 Abs. 4 TKG). Danach sind grundsätzlich auch die Betreiber sogenannter geschlossener Benutzergruppen und Corporate Networks betroffen. Das Telekommunikationsgesetz gibt dem Verordnungsgeber aber die Möglichkeit zu bestimmen, bei welchen Telekommunikationsanlagen technische Einrichtungen zur Umsetzung von Abhörmaßnahmen nicht zu gestalten oder vorzuhalten sind. Dies ist insbesondere für

Telekommunikationsanlagen in Arztpraxen, Rechtsanwaltskanzleien und Redaktionsbüro von Bedeutung, bei denen besondere Berufsgeheimnisse zu wahren sind. Gleichwohl werden damit keine „abhörfeien Zonen“ geschaffen.

Das Surfen im Internet darf nicht Gegenstand von TK-Überwachungsmaßnahmen sein. Nach deutschem Recht dürfen nur die folgenden über das Internet abgewickelten Dienste abgehört werden, weil es sich insoweit um Telekommunikationsdienste handelt:

- E-Mail-Kommunikation
- Internettelefonie
- SMS (Short Message Service)
- Mailboxsysteme.

Aus Sicht des Datenschutzes ist es wichtig, dass die verpflichteten Telekommunikationsunternehmen die vorgelegten Anordnungsbeschlüsse auf Telekommunikationsüberwachung auf die Beachtung der einschlägigen formalen Vorgaben überprüfen dürfen/müssen (z.B. Angabe einer Katalogstraftat nach § 100a StPO).

Zum Entwurf der TKÜV hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10.05.2001 eine Entschließung verabschiedet (siehe Anhang 7).

3 Grundsätze des Datenschutzrechts

3.1 Vorrang bereichsspezifischer Datenschutzregelungen

Um die Interessen der Nutzer von Telekommunikationsdiensten hinsichtlich ihrer persönlichen Daten angemessen zu schützen, sind mittlerweile eine Vielzahl von Datenschutzregelungen geschaffen worden. Wesentliches Schutzgut und damit Ausgangspunkt für Regelungsinhalt und -tiefe dieser Bestimmungen ist das Recht auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht in dem so genannten Volkszählungsurteil aus dem Jahr 1983 beschrieben hat. Danach muss der Einzelne in die Lage versetzt werden, sich seine Privatsphäre zu erhalten, um zu verhindern, dass er deshalb in zunehmende Abhängigkeit von Stellen in Staat und Wirtschaft gerät, weil diese immer mehr von ihm wissen (wollen).

Auf der anderen Seite benötigt der moderne Rechts- und Sozialstaat in großem Umfang personenbezogene Daten, um seine vielfältigen Aufgaben sachlich richtig und gerecht erfüllen zu können. Auch in Bezug auf die legitimen Interessen der Wirtschaft kann das Recht auf informationelle Selbstbestimmung nicht grenzenlos sein. Dem Einzelnen kann daher kein Recht im Sinne einer absoluten, uneingeschränkten Herrschaft über seine Daten zugesprochen werden. Einschränkungen des Datenschutzes sind nach den Vorgaben des Volkszählungsurteils allerdings nur im überwiegenden Allgemeininteresse zulässig. Darüber hinaus bedürfen derartige Einschränkungen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entsprechen muss.

Die Verarbeitung personenbezogener Daten kann daher nicht mit einigen wenigen entsprechend allgemein gehaltenen Vorschriften geregelt werden. Nach den Vorgaben des Bundesverfassungsgerichts sind Bestimmungen erforderlich, die jeweils einen bestimmten datenschutzrelevanten Lebenssachverhalt reflektieren, diesen regeln und dabei das Recht des Einzelnen auf informationelle Selbstbestimmung angemessen zu berücksichtigen haben. Der Schwerpunkt des Datenschutzrechts ist damit auf den sog. bereichsspezifischen Teil der Gesetzgebung verlagert worden. Den Bestimmungen des Bundesdatenschutzgesetzes kommt vor diesem Hintergrund lediglich eine Auffangfunktion zu. Dies erklärt die vielen in bereichsspezifischen Datenschutzregelungen enthaltenen Verweise und Bezugnahmen auf das Bundesdatenschutzgesetz, so z.B. in § 1 Abs. 2 TDSV.

3.2 Verbot mit Erlaubnisvorbehalt

Für die Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein Verbot mit Erlaubnisvorbehalt. In diesem Sinne bestimmt § 4 Abs. 1 BDSG, dass die Erhebung, Verarbeitung sowie die Nutzung personenbezogener Daten grundsätzlich verboten sind, es sei denn,

- sie werden durch das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder
- der Betroffene erklärt dazu seine Einwilligung.

Entsprechende Vorschriften für die Erhebung und die Verarbeitung personenbezogener Daten sowie deren sonstige Nutzung enthält auch das bereichsspezifische Datenschutzrecht in der Telekommunikation. So dürfen nach § 3 Abs. 1 TDSV die Diensteanbieter „für Telekommunikationszwecke

personenbezogene Daten der am Fernmeldeverkehr Beteiligten nur erheben, verarbeiten und nutzen, soweit diese Verordnung oder andere Rechtsvorschriften es erlauben oder der Beteiligte eine Einwilligung erteilt hat,...“.

Für die dem Fernmeldegeheimnis unterliegenden personenbezogenen Daten ist der Grundsatz vom Erlaubnisvorbehalt in § 85 Abs. 3 TKG noch verschärft worden. Diese Daten dürfen für andere Zwecke, insbesondere für die Weitergabe an Dritte, nur dann verwendet werden, soweit das Telekommunikationsgesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Datenschutzrechtlich problematisch sind danach beispielsweise Vorschriften aus dem Handelsrecht, wonach der Handelsvertreter, der für einen Mobilfunknetzbetreiber Verträge über Telekommunikationsdienstleistungen abschließt, im Falle einer vereinbarten Umsatzprovision berechtigt ist, Kenntnis von den für die Umsatzhöhe maßgeblichen Verbindungsdaten nehmen darf. Soweit diese und vergleichbare Regelungen einschlägig sind, ist der Gesetzgeber aufgefordert, die entsprechenden Bestimmungen den Vorgaben des § 85 Abs. 3 TKG anzupassen.

3.3 Einwilligung des Betroffenen

Soweit eine Rechtsvorschrift die Verarbeitung personenbezogener Daten, die dem Fernmeldegeheimnis unterliegen, ausdrücklich erlaubt oder sogar anordnet, bleibt für eine Einwilligung des Betroffenen kein Raum. In diesen Fällen ist die entsprechende Nutzung personenbezogener Daten grundsätzlich auch gegen den Willen des Betroffenen zulässig. Dies gilt beispielsweise für die in § 89 Abs. 6 TKG vorgesehene Übermittlung von Kundendaten durch Telekommunikationsdiensteanbieter an Strafverfolgungs- und Sicherheitsbehörden.

Ist die Verarbeitung personenbezogener Daten demgegenüber nicht in einer Rechtsnorm verbindlich vorgesehen, bedarf es insoweit einer entsprechenden Einwilligung, d.h. einer vorherigen Einverständniserklärung des Betroffenen. Die Wirksamkeit der Einwilligung hängt dabei im Wesentlichen von der Freiwilligkeit der getroffenen Entscheidung ab. Der Betroffene darf nicht den Eindruck gewinnen, er habe letztlich keine andere Wahl, als einer Verarbeitung seiner Daten zuzustimmen. Dies gilt insbesondere dann, wenn dem Betroffenen das Gefühl vermittelt wird, dass ihm die Einwilligung unter Ausnutzung einer wirtschaftlichen Machtposition quasi „abgepresst“ wird.

Für die Frage der Entscheidungsfreiheit bei der Abgabe einer Einwilligungserklärung ist im Telekommunikationsbereich die Regelung des § 89 Abs. 10 Satz 1 TKG von

Bedeutung. Danach darf die geschäftsmäßige Erbringung von Telekommunikationsdiensten und deren Entgeltfestlegung nicht von der Angabe personenbezogener Daten abhängig gemacht werden, die für die Erbringung oder Entgeltfestlegung dieser Dienste nicht erforderlich sind. So sind beispielsweise Fragen zur Religionszugehörigkeit nicht zulässig.

Die Einwilligung eines Nutzers von Telekommunikationsdiensten ist weiterhin nur wirksam, wenn sich der Einwilligende über die Tragweite seiner Entscheidung bewusst ist. Im Ergebnis heißt dies, dass der Betroffene in der Lage sein muss, das ihm zustehende Recht auf informationelle Selbstbestimmung im konkreten Fall eigenverantwortlich ausüben zu können. Eine hierfür maßgebliche Vorschrift stellt § 3 Abs. 5 TDSV dar. Danach sind die Telekommunikationsdiensteanbieter verpflichtet, konkret und umfassend ihre Kunden sowie die übrigen Nutzer über die Verarbeitung und Nutzung personenbezogener Daten zu informieren. Ziel dieser Vorschrift ist es, eine möglichst große Transparenz der Datenverarbeitungsvorgänge für die Nutzer von Telekommunikationsdiensten sicherzustellen. Von besonderer Bedeutung ist dabei, dass nach § 3 Abs. 5 TDSV die Kunden auch auf die möglichen Gestaltungs- und Wahlmöglichkeiten aufmerksam gemacht werden müssen, auch wenn sie diese nicht selbst ansprechen. Einschlägig ist diese Bestimmung für die Wahl der Rechnungsart sowie für die Fragen nach einem Eintrag von Kundendaten in öffentliche Kundenverzeichnisse bzw. deren Aufnahme in einen telefonischen Auskunftsdienst.

Gemäß § 4a Abs. 1 Satz 3 BDSG bedarf die Einwilligung in der Regel der Schriftform. Für den Bereich der Telekommunikation findet dieser allgemeine Grundsatz seine bereichsspezifische Ausprägung in § 89 Abs. 10 Satz 4 TKG, der für die Wirksamkeit der datenschutzrechtlichen Einwilligungserklärung ebenfalls die Schriftform voraussetzt.

Mit § 4 TDSV wird die in § 89 Abs. 10 TKG vorgesehene Befugnis des Kunden, eine Einwilligung auch in elektronischer Form abgeben zu können, näher ausgestaltet. Vorbild für diese Regelung ist § 3 Abs. 7 Teledienstedatenschutzgesetz, dem § 4 Nr. 1 bis 4 TDSV entspricht. Die in § 4 Nr. 4 TDSV vorgesehene Widerrufsmöglichkeit beruht auf § 89 Abs. 10 Satz 5 TKG, wobei die Dauer der Rücknahmemöglichkeit von einer Woche § 1 Haustürwiderrufsgesetz nachgebildet ist.

Für den Abschluss von Verträgen über Telekommunikationsdienstleistungen werden seitens der anbietenden Unternehmen in der Regel vorformulierte Auftragsvordrucke verwendet. Diese enthalten auch datenschutzrechtlich relevante

Einwilligungserklärungen, wie z.B. die Einwilligung in eine Anfrage bei einer Wirtschaftsauskunftei oder das Einverständnis mit einer Eintragung telekommunikationsrelevanter Daten in öffentliche Kundenverzeichnisse. Hierbei ist darauf zu achten, dass die einzelne Einwilligungserklärung im äußeren Erscheinungsbild des Auftragsformulars drucktechnisch hervorgehoben wird, so dass der Betroffene ohne größere Schwierigkeiten Inhalt und Umfang seiner Erklärung erkennen kann. Unzulässig ist es demgegenüber, die Einwilligung bei Formularverträgen im sog. „Kleingedruckten“ zu verstecken, so dass sich der Betroffenen gar nicht bewusst ist, auch diese Einwilligungserklärung abgegeben zu haben. Aus diesem Grunde genügt auch ein bloßer Hinweis auf die Allgemeinen Geschäftsbedingungen den datenschutzrechtlichen Anforderungen nicht.

Etwas anderes gilt gemäß § 4a Abs. 1 Satz 3 BDSG nur dann, wenn ein Verzicht auf die Schriftform aufgrund der besonderen Umstände des Einzelfalles gerechtfertigt und angemessen erscheint. Damit die infrage stehende Verarbeitung personenbezogener Daten zulässig ist, muss die insoweit notwendige mündliche Einwilligung ausdrücklich erklärt werden. Weder eine konkludente noch eine mutmaßliche Einwilligung reichen insoweit. Aufgrund der Systematik von § 4a Abs. 1 BDSG bzw. § 89 Abs. 10 TKG handelt es sich bei der mündlich erklärten Einwilligung um eine möglichst restriktiv anzuwendende Alternative zur schriftlichen Einwilligung. Gerade im Bereich der Telekommunikation gewinnt diese Frage verstärkt an Bedeutung, da die sog. Call-Center nicht nur für das Beschwerdemanagement der Telekommunikationsdiensteanbieter eingesetzt werden, sondern vermehrt auch zur Beauftragung von Telekommunikationsdienstleistungen. Viele Kunden möchten heutzutage ihren Telefonvertrag fernmündlich abschließen und sind nicht bereit, hierzu ein Ladenlokal aufzusuchen. Dies gilt in gleicher Weise auch für die mittlerweile bei einigen Telekommunikationsdiensteanbietern übliche Online-Auftragsbearbeitung, bei der ebenfalls auf einen Papierauszug des Vertrages verzichtet wird. Will man diesen Umständen angemessen Rechnung tragen und auf eine schriftliche Einwilligungserklärung verzichten, so muss zumindest sichergestellt werden, dass durch die Versendung eines Bestätigungsschreibens an den Kunden dieser im nachhinein über seine Einwilligung(en) informiert wird. Darüber hinaus ist es notwendig, dem Kunden eine ausreichende Frist zu setzen, innerhalb der Einwendungen geltend gemacht werden können. Auf diesem Weg können auch Missverständnisse in einem für alle Beteiligten zumutbaren Verfahren bereinigt werden.

Zusammenfassend ist für die Fälle, in denen eine Verarbeitung oder Nutzung personenbezogener Daten nur aufgrund einer entsprechenden Einwilligung des Betroffenen zulässig ist, folgendes zu beachten:

- Der Betroffene ist vorher über Inhalt und Reichweite seiner Einwilligung aufzuklären.
- Die Einwilligung muss unbelastet sein, d.h. die Versagung der Einwilligung darf nur in besonderen Fällen und nicht zwangsläufig zur Ablehnung eines Vertragsabschlusses führen.
- Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

3.4 Rechte des Betroffenen

Das Datenschutzrecht stellt denjenigen, deren personenbezogene Daten durch Dritte erhoben, verarbeitet oder genutzt werden, Instrumente zur Verfügung, um ihr Recht auf informationelle Selbstbestimmung sicherzustellen. Dabei handelt es sich im Bereich der nicht öffentlichen Datenverarbeitung nach dem Bundesdatenschutzgesetz um

- das Auskunftsrecht nach § 34 BDSG sowie
- die Rechte auf
    - Berichtigung nach § 35 Abs. 1 BDSG,
    - Löschung nach § 35 Abs. 2 BDSG,
    - Sperrung nach § 35 Abs. 3 BDSG.

Zu beachten ist, dass diese Rechte nach § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft, d.h. durch Vertrag ausgeschlossen oder beschränkt werden können. Weitere Einzelheiten siehe 3.4.1 bzw. 3.4.3).

Zudem besteht in bestimmten Fällen ein Anspruch auf Benachrichtigung (3.4.2). Schließlich kann der Bundesbeauftragte für den Datenschutz angerufen werden (siehe 3.4.4) und vor Gericht das Recht auf Schadensersatz eingeklagt werden (siehe 3.4.5).

3.4.1 Das Recht auf Auskunft

Das Telekommunikationsgesetz enthält keine spezielle Vorschrift zum Auskunftsrecht des Betroffenen. Damit gilt hier das Bundesdatenschutzgesetz.

Danach hat grundsätzlich jeder - unabhängig von Alter, Wohnsitz und Nationalität - ein Recht auf Auskunft

- über die zu seiner Person gespeicherten Daten,
- über die Herkunft der Daten,
- über den Empfänger der Daten,
- über den Zweck der Speicherung und
- über Personen und Stellen, an die regelmäßig übermittelt wird (gilt nur bei automatisierter Verarbeitung).

Bei Auskunftsersuchen sollte folgendes beachtet werden:

- Es empfiehlt sich, die Auskunft schriftlich anzufordern. Zur Legitimation genügt es in der Regel, die Kopie eines Personaldokuments beizulegen. Einschreiben ist nicht erforderlich.
- Bei persönlicher Vorsprache wird eine sofortige Erledigung oft nicht möglich sein.
- Bei telefonischen Auskunftsersuchen kann der Anrufer meist nicht sicher identifiziert werden. Deshalb gilt der Grundsatz: Keine telefonische Datenauskunft.
- Die gewünschte Auskunft ist möglichst genau zu bezeichnen.
- Das Auskunftsersuchen ist an den Vertragspartner oder direkt an die Stelle zu richten, von der vermutet wird, dass dort personenbezogene Daten des Betroffenen gespeichert sind.

Die Auskunft ist kostenlos.

Bei Zweifeln, ob korrekt Auskunft erteilt worden ist, kann sich der Betroffene an den Bundesbeauftragten für den Datenschutz wenden. Der Schriftwechsel sollte in Kopie beigefügt werden.

Außerdem besteht die Möglichkeit einer gerichtlichen Klage.

Wer mehr zu seinem Auskunftsrecht nach dem Bundesdatenschutzgesetz wissen möchte, sollte die BfD-Info 1 anfordern (siehe Anhang 8) oder die Website des Bundesbeauftragten für den Datenschutz besuchen (dort: Datenschutz von A-Z, Auskunft - siehe Anhang 9).

3.4.2 Das Recht auf Benachrichtigung

Jede nicht-öffentliche Stelle ist verpflichtet, alle Betroffenen, über die sie Daten ohne deren Kenntnis verarbeitet, individuell zu benachrichtigen (§ 33 BDSG).
Die Benachrichtigung muss umfassen:

- Angabe der speichernden Stelle mit Name/Firma und Anschrift,
- die Tatsache, dass erstmals Daten über die Person, die benachrichtigt wird, gespeichert oder übermittelt werden, und
- die Art der Daten.

Es gibt nach § 33 Abs. 2 BDSG allerdings Ausnahmen von der Pflicht zur Benachrichtigung, so etwa, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung seiner Daten erlangt hat oder die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist. Weitere Einzelheiten können Sie der BfD-Info 1 entnehmen (siehe Anhang 8).

Die allgemeine Benachrichtigungspflicht wird im Bereich des Telekommunikationsdatenschutzrechts noch durch eine allgemeine Informationsverpflichtung der Anbieter von Telekommunikationsdiensten ergänzt. Nach der bereichsspezifischen Regelung des § 3 Abs. 5 TDSV sind die Kunden von Telekommunikationsdiensteanbietern bei Vertragsschluss über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten so unterrichten, dass sie in allgemein verständlicher Form Kenntnis von den zugrundliegenden Verarbeitungstatbeständen der Daten erhalten. Zur Konkretisierung dieser Informationspflicht hat der Bundesbeauftragte für den Datenschutz sogenannte Guidelines zur Kundeninformation entwickelt (siehe Anhang 3).

3.4.3 Die Rechte auf Berichtigung, Löschung oder Sperrung

Für die in Bezug auf die Datenverarbeitung im nicht-öffentlichen Bereich gemäß § 35 BDSG vorgesehenen Rechte auf Berichtigung, Löschung und Sperrung gibt es nur teilweise vorrangige Bestimmungen im Telekommunikationsgesetz oder in der Telekommunikations-Datenschutzverordnung. Insofern sind die allgemeinen Vorschriften des Bundesdatenschutzgesetzes durchaus wichtig: Jede Stelle ist verpflichtet, unrichtige Daten zu berichtigen. Es liegt aber auch am Betroffenen selbst, darauf hinzuweisen, wenn Daten unrichtig oder überholt sind.

Von nicht öffentlichen Stellen sind personenbezogene Daten zu löschen, wenn

- die Speicherung unzulässig ist, etwa weil sie im Vertrag nicht vorgesehen war, oder
- es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über die Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und die speichernde Stelle deren Richtigkeit nicht beweisen kann, oder
- für eigene Zwecke verarbeitete Daten für die Erfüllung des Speicherungszwecks nicht mehr erforderlich sind, oder
- geschäftsmäßig zum Zweck der Übermittlung verarbeitete Daten aufgrund einer am Ende des fünften Kalenderjahres nach der ersten Speicherung vorzunehmenden Prüfung nicht mehr erforderlich sind.

Eine Löschung ist nur für personenbezogene Daten vorgesehen, die in einer Datei verarbeitet werden, jedoch nicht für einzelne Daten, die in Akten festgehalten sind. Im Telekommunikationsbereich ist die bereichsspezifische Vorschrift des § 5 Abs. 3 TDSV zu beachten, wonach die Bestandsdaten (siehe 4.5.1.2) - von Ausnahmefällen abgesehen - mit Ablauf des Jahres zu löschen sind, das auf die Beendigung des Vertragsverhältnisses mit einem Anbieter von Telekommunikationsdiensten folgt. Zur Löschung von Verbindungsdaten siehe 4.5.3.1.

Personenbezogene Daten sind zu sperren, wenn der Betroffene ihre Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Sie sind immer dann zu sperren, wenn einer fälligen Löschung besondere Gründe entgegenstehen, etwa

- gesetzlich, satzungsmäßig oder vertraglich festgelegte Aufbewahrungsfristen,
- schutzwürdige Interessen des Betroffenen, etwa weil ihm Beweismittel verloren gingen, oder
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

3.4.4 Das Recht auf Anrufung des Bundesbeauftragten für den Datenschutz und anderer Kontrollinstitutionen

Wer annimmt, bei der Erhebung, Verarbeitung oder Nutzung seiner persönlichen Daten durch eine nicht-öffentliche Stelle in seinen Rechten verletzt worden zu sein, kann sich nach den §§ 21 bzw. 38 BDSG an eine Datenschutzkontrollinstitution wenden (zu den einzelnen Kontrollzuständigkeiten siehe 4.8). Für die geschäftsmäßig erbrachten Telekommunikationsdienste ist dies gemäß § 91 Abs. 4 TKG der Bundesbeauftragte für den Datenschutz. Falls Sie also Probleme mit dem Telekommunikationsdiensteanbieter haben, bei dem Sie Kunde sind, können Sie sich an den Bundesbeauftragten wenden.

Alle Eingaben werden vertraulich behandelt. Auf Wunsch des Betroffenen bleibt sein Name auch gegenüber der Stelle ungenannt, über die er sich beschwert, falls seine Beschwerde dort zu einer Nachfrage führt und sein individuelles Problem ohne Nennung des Namens zu klären ist.

Die Anschriften und Telefonnummern der Datenschutzbeauftragten des Bundes und der Länder sowie der Aufsichtsbehörden für den nicht-öffentlichen Bereich können den Anhängen 10 und 11 entnommen werden.

3.4.5 Das Recht auf Schadensersatz

Da weder das Telekommunikationsgesetz noch andere Vorschriften des Telekommunikationsrechts besondere Regelungen zum Schadensersatz enthalten, gelten die grundsätzlichen Regelungen des Bundesdatenschutzgesetzes (§§ 7, 8 BDSG). Durch eine über die Haftung nach dem Bürgerlichen Gesetzbuch hinausgehende Verpflichtung zum Schadensersatz bei unrichtiger oder unzulässiger automatisierter Datenverarbeitung verbessert das BDSG den Schutz des Persönlichkeitsrechts, auch indem es die datenverarbeitenden Stellen zu besonderer Sorgfalt beim Umgang mit personenbezogenen Daten anhält.

Öffentliche Stellen haften nach dem Prinzip der Gefährdungshaftung, d.h. sie sind unabhängig von einem Verschulden zum Ersatz des Schadens verpflichtet (bis höchstens 130.000 EUR). Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen zudem auch der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen (Schmerzensgeld).

Bei der Geltendmachung eines Schadensersatzanspruchs gegenüber einer nicht-öffentlichen Stelle wie einem Telekommunikationsdiensteanbieter hilft das Gesetz

dem Geschädigten durch eine Beweislastumkehr. Wenn streitig ist, ob der Schaden die Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, so muss diese beweisen, dass das nicht der Fall ist. Im Übrigen finden die Regelungen des Bürgerlichen Gesetzbuches zum Schadensersatz Anwendung.

3.4.6 Straf- und Bußgeldvorschriften

Das Telekommunikationsrecht enthält einige spezielle Straf- und Bußgeldvorschriften, die allerdings nicht alle datenschutzrelevante Punkte betreffen.

Für den Schutz des Fernmeldegeheimnisses ist bedeutend, dass gem. § 95 TKG mit einer Freiheitsstrafe bedroht wird, wer mit einer Funkanlage eine Nachricht abhört, die nicht für diese bestimmt war (siehe 4.3).

Bußgeldtatbestände enthält § 17 TDSV. Die Fälle, die bei vorsätzlichem oder fahrlässigem Handeln eine Ordnungswidrigkeit sind und mit einem Bußgeld geahndet werden können, sind folgende:

1. Nutzung der Bestandsdaten für Zwecke der Beratung, Werbung und Marktforschung ohne Einwilligung des Kunden;
2. Speicherung der Verbindungsdaten über das Ende der Verbindung hinaus, obwohl sie nicht mehr erforderlich sind;
3. Verarbeitung und Nutzung der Verbindungsdaten zur bedarfsgerechten Gestaltung eines Telekommunikationsdienstes ohne Einwilligung des Kunden oder ohne Anonymisierung der Daten des Angerufenen;
4. Löschung der Verbindungsdaten nicht rechtzeitig oder gar nicht;
5. Löschung der Daten und Belege im Telegrammdienst erfolgt nicht rechtzeitig.

Zuständige Behörde für die Verhängung eines Bußgeldes ist nach § 96 Abs. 2 TKG die Regulierungsbehörde für Telekommunikation und Post.

4 Datenschutz in der Telekommunikation: Das Telekommunikationsgesetz und die Telekommunikations-Datenschutzverordnung

4.1 Anwendungsbereich

Die für den Datenschutz in der Telekommunikation einschlägigen Vorschriften des Elften Teils des Telekommunikationsgesetzes sowie die Bestimmungen der Telekommunikations-Datenschutzverordnung richten sich grundsätzlich an Personen oder Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen. Zum geschäftsmäßigen Erbringen von Telekommunikationsdiensten gehört das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte (§ 3 Nr. 5 TKG). Dabei ist es unerheblich, ob diese Tätigkeit mit oder ohne Gewinnerzielungsabsicht ausgeübt wird. Ohne Bedeutung ist zudem, ob der fragliche Telekommunikationsdienst der Öffentlichkeit gegenüber oder nur für bestimmte Dritte angeboten wird. Die datenschutzrechtlichen Vorschriften sind deshalb nicht nur auf „Telefongesellschaften“ sondern auch auf „geschlossene Benutzergruppen“ anzuwenden. Dies sind neben sogenannten Corporate Networks (d.h. geschlossene Benutzergruppen, die nicht für jedermann öffentlich zugänglich sind, wie z.B. Netzwerke von Unternehmen oder Behörden) auch Telekommunikationsanlagen in Hotels und Krankenhäusern, soweit sie den Beschäftigten, Gästen usw. auch zur privaten Nutzung zur Verfügung gestellt werden.

Auch die Telekommunikationsdienstleistung stellt das Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte dar. Im Gegensatz zum Telekommunikationsdienst wird eine Telekommunikationsdienstleistung i.S.d. § 3 Nrn. 18, 19 TKG jedoch stets gewerblich, d.h. mit Gewinnerzielungsabsicht betrieben. Dabei unterscheidet das Gesetz im Fall der Telekommunikationsdienstleistung zwischen Telekommunikationsdienstleistungen, die der Öffentlichkeit gegenüber, d.h. für beliebige natürliche oder juristische Personen (§ 3 Nr. 19 TKG) oder nur für die Teilnehmer geschlossener Benutzergruppen (§ 3 Nr. 18 TKG) angeboten werden.

Weder im Fall des § 3 Nr. 5 TKG noch beim Anwendungsbereich des § 3 Nr. 18 bzw. 19 TKG muss der Diensteanbieter selbst über die notwendige technische Infrastruktur verfügen.

4.2 Fernmeldegeheimnis

Der verfassungsrechtliche Schutz des Fernmeldegeheimnisses in Art. 10 GG gewährleistet dem Einzelnen, Nachrichten und Informationen unbeobachtet von der Öffentlichkeit austauschen zu können. Eingriffe sind nur aufgrund eines Gesetzes zulässig. Dabei betrifft Art 10 GG aber ausschließlich das Verhältnis zwischen Bürger und Staat. Nach der Liberalisierung des Telekommunikationsmarktes war es notwendig geworden, das Fernmeldegeheimnis auch im Verhältnis zwischen Anbietern und Nutzern von Telekommunikationsdiensten sicher zu stellen.

Anders als Art. 10 GG schützt § 85 TKG vor unbefugten Eingriffen derjenigen Privatpersonen oder -unternehmen, die Telekommunikationsdienste erbringen oder daran mitwirken. Auch diesen ist es untersagt, „sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen“ und diese Kenntnis für andere Zwecke zu verwenden (§ 85 Abs. 3 TKG). Dabei gilt das Fernmeldegeheimnis nach § 85 TKG nicht nur für gewerbliche Anbieter von Telekommunikationsdienstleistungen, sondern für alle, die geschäftsmäßig Telekommunikationsdienste (siehe 4.5.1.2) erbringen.

Geschützt ist das Interesse des einzelnen, sowohl den Inhalt als auch die näheren Umstände der Telekommunikation geheim zu halten. Mit „Inhalt“ sind die mittels Telekommunikationsanlagen übermittelten individuellen Nachrichten, mit dem Begriff „nähere Umstände“ insbesondere die Verbindungsdaten (siehe 4.5.1.2) eines Kommunikationsvorgangs gemeint. Es wird klargestellt, dass auch erfolglose Verbindungsversuche, also z.B. die Tatsache, dass jemand vergeblich versucht hat, jemand anderen anzurufen, dem Fernmeldegeheimnis unterliegen (§ 85 Abs. 1 TKG).

Nicht unter den Schutz des Fernmeldegeheimnisses fallen dagegen in der Regel private Endgeräte, Haustelefonanlagen und hauseigene Sprechanlagen.

4.3 Abhörverbot

Das Abhörverbot nach § 86 TKG untersagt, mit Funkgeräten Sendungen abzuhören, die für den Abhörenden nicht bestimmt sind. Hierzu zählen z.B. auch die mit Hilfe von schnurlosen Telefonen geführten Gespräche, die, soweit sie noch mit analoger Übertragungstechnik arbeiten, mit Funkempfängern (Breitbandempfänger, „Scanner“

usw.) abgehört werden können. Verstöße hiergegen werden gemäß § 95 TKG mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe geahndet (siehe 3.4.6).

4.4 Technische Schutzmaßnahmen

Nach § 87 Abs. 1 TKG haben alle Telekommunikationsunternehmen beim Betrieb ihrer Telekommunikations- und Datenverarbeitungssysteme „angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

- des Fernmeldegeheimnisses und personenbezogener Daten,
- der programmgesteuerten Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe,
- gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und
- von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen.“

Die Erfüllung dieser Verpflichtung kann gemäß § 87 Abs. 3 TKG durch Rechtsverordnung geregelt werden. Das Bundesministerium für Wirtschaft und Technologie beabsichtigt, von dieser Verordnungsermächtigung solange keinen Gebrauch zu machen, wie Telekommunikationsunternehmen aus eigenem Antrieb ausreichende Schutzmaßnahmen ergreifen. Dabei soll ihnen der gemäß § 87 Abs. 1 TKG von der Regulierungsbehörde für Telekommunikation und Post im Benehmen mit dem Bundesamt für die Sicherheit in der Informationstechnik erstellte „Katalog von Sicherheitsanforderungen“ Hilfestellung leisten.

Der Katalog kann bei der

Regulierungsbehörde für Telekommunikation und Post (Reg TP)
Referat Z 24-DrV
Canisiusstr. 21b
55122 Mainz

bestellt werden oder von der

Bundesanzeiger Verlagsgesellschaft mbH,
Postfach 13 20,
53003 Bonn,

als Beilage Nr. 208 a des Bundesanzeigers von 1997 bezogen werden. Er ist ferner im Internetangebot der Regulierungsbehörde für Telekommunikation und Post (http://www.regtp.de. - dort unter „Druckschriften“) als PDF-Datei verfügbar. Praktische Bedeutung für den Bürger kann dieser Katalog beispielsweise bei Sicherheitsaspekten von Verteilern in Mehrfamilienhäusern haben.

4.5 Bereichsspezifische Datenschutzvorschriften

4.5.1 Grundsätzliches zur Datenerhebung, - verarbeitung und -nutzung durch Telekommunikationsdiensteanbieter

4.5.1.1 Zulässiger Umfang des Umgangs mit Kundendaten

Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, dürfen nach § 89 Abs. 2 TKG Daten natürlicher und juristischer Personen erheben, verarbeiten und nutzen, soweit dies erforderlich ist

- zur betrieblichen Abwicklung geschäftsmäßiger Telekommunikationsdienste,

- zu deren bedarfsgerechter Gestaltung sowie

- auf Antrag des Nutzers (Kunden) zur Darstellung von Leistungsmerkmalen (insbesondere für den Entgeltnachweis) und

- auf Antrag des Nutzers (Kunden) zur Identifizierung von Anschlüssen (sog. Fangschaltungen).

Nähere Regelungen hierzu enthält die auf der Grundlage von § 89 Abs. 1 TKG erlassene TDSV. Darin wird auch weiter konkretisiert, um welche Daten es sich hierbei handelt, nämlich Bestandsdaten, Verbindungsdaten und weitere für die Abrechnung von Telekommunikationsdiensten erforderliche Daten (Entgeltdaten). Zur Erläuterung der einzelnen Datenarten siehe 4.5.1.2.

4.5.1.2 Begriffserläuterungen

Bestandsdaten sind personenbezogene Daten eines an der Telekommunikation Beteiligten, die erhoben werden, um ein Vertragsverhältnis über Telekommunikationsdienste einschließlich dessen inhaltlicher Ausgestaltung mit dem Diensteanbieter zu begründen oder zu ändern, also z.B. Name, Anschrift, Kontonummer usw. (§ 5 Abs. 1 Satz 1 i.V.m. § 2 Nr. 3 TDSV).

Beteiligte an der Telekommunikation sind die Vertragspartner (Kunden) bei Verträgen über Telekommunikationsdienste mit einem Diensteanbieter sowie alle Personen, die die von einem Diensteanbieter angebotenen Telekommunikationsdienste nutzen (§ 2 Nr. 1 TDSV).

Diensteanbieter sind alle, die ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken (§ 2 Nr. 2 TDSV), z.B. Sprachtelefondienst, Datenübertragung usw.. Die Diensteanbieter müssen nicht über eigene Netze verfügen.

Entgeltdaten sind die Daten, die für die Tarifierung, die Rechnungserstellung, den Rechnungsversand (§ 7 Abs. 2 Nr. 2 TDSV) sowie die Abrechnungsbuchführung (§ 7 Abs. 2 Nr. 3 TDSV) benötigt werden.

Geschäftsmäßiges Erbringen von Telekommunikationsdiensten ist das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht (§ 3 Nr. 5 TKG). Diese Voraussetzung erfüllen auch Unternehmen und Behörden, die ihren Beschäftigten erlauben, über die eigene Telekommunikationsanlage privat zu telefonieren.

Kundenkarten sind Karten, mit deren Hilfe Telekommunikationsverbindungen hergestellt und personenbezogene Daten erhoben werden können (§ 2 Nr. 5 TDSV). Von datenschutzrechtlicher Bedeutung ist, dass die Kartennummer zu den Verbindungsdaten im Sinne von § 6 Abs. 1 Nr. 1 TDSV gehört.

Telekommunikation ist der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen (§ 3 Nr. 16 TKG).

Telekommunikationsanlagen sind technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden,

übertragen, vermitteln, empfangen, steuern oder kontrollieren können (§ 3 Nr. 17 TKG).

Verbindungsdaten sind die personenbezogenen Daten eines an der Telekommunikation Beteiligten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden. Es handelt sich um Daten, die sich auf die einzelnen Telekommunikationsverbindungen beziehen, wie z.B. Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses, Beginn und Ende der jeweiligen Verbindung nach Datum und Uhrzeit, Art des in Anspruch genommenen Telekommunikationsdienstes (z.B. Fax, Datenübertragung), Endpunkte von festgeschalteten Verbindungen sowie ihren Beginn und ihr Ende nach Datum und Uhrzeit, und sonstige zum Aufbau oder zur Aufrechterhaltung einer Verbindung sowie zur Entgeltberechnung notwendige Verbindungsdaten (§ 6 Abs. 1 i.V.m. § 2 Nr. 5 TDSV).

Die Begriffe Erheben, Verarbeiten und Nutzen werden im Telekommunikationsrecht mit der gleichen Bedeutung verwendet wie im BDSG (nähere Erläuterungen enthält die Broschüre BfD-Info 1, siehe Anhang 8).

4.5.1.3 Zweckbindung und Verhältnismäßigkeit

Die Vorschriften über den Umgang mit telekommunikationsrelevanten Daten orientieren sich

- am Grundsatz der Zweckbindung (d.h., dass sie ohne ausdrückliche Einwilligung des Betroffenen nicht für andere als die in bereichsspezifischen Datenschutzregelungen für die Telekommunikation erlaubten Zwecke verwendet werden dürfen) und

- am Grundsatz der Verhältnismäßigkeit, insbesondere also der Beschränkung des Umgangs mit diesen Daten auf das Erforderliche.

Zum Umgang mit Bestandsdaten siehe insbesondere 4.5.2. Der Umgang mit Verbindungsdaten wird in 4.5.3 bis 4.5.7 beschrieben.

4.5.2 Telekommunikationsverträge

Seit der Liberalisierung des Telekommunikationsmarktes werden sämtliche Telekommunikationsdienste zwischen den Kommunikationsdiensteanbietern und ihren Kunden vertraglich vereinbart. Diesen Verträgen liegen regelmäßig sog. „Allgemeine Geschäftsbedingungen“ (AGB) zugrunde.

Neben der Festlegung der zu erbringenden Telekommunikations-Dienstleistung (z.B. ISDN-Telefonanschluss im Festnetz) und dem dafür zu zahlenden Entgelt müssen die nach den datenschutzrechtlichen Vorschriften erforderlichen Vereinbarungen getroffen werden. Nach § 3 Abs. 5 TDSV haben die Diensteanbieter ihre Kunden bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten so zu unterrichten, dass die Kunden in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Dabei sind die Kunden auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Hierzu gehören insbesondere die Wünsche der Kunden in Bezug auf die Aufnahme ihrer Daten in öffentliche Kundenverzeichnisse und telefonische Auskunftsdienste. Die Vorschrift betrifft auch Fragen zur Speicherung und Darstellung ihrer detaillierten Gesprächsdaten, den sog. Verbindungsdaten (siehe 4.5.3.1) sowie Hinweise und Einwilligung zur Bonitätsprüfung (siehe 4.5.2.4).

Um den Diensteanbietern eine entsprechende Hilfestellung zu geben, haben der Bundesbeauftragte für den Datenschutz und die Regulierungsbehörde für Telekommunikation und Post gemeinsam sog. „Guidelines“ zu den wesentlichen datenschutzrechtlichen Fragen erarbeitet. Diese sind gleichermaßen als Information für die Kunden bedeutsam, weil sie dadurch für die wesentlichen datenschutzrechtlichen Fragen sensibilisiert werden und die Qualität der Vertragsgestaltung ihres Diensteanbieters beurteilen können. Die Guidelines sind im Anhang 3 abgedruckt.

4.5.2.1 Wahlrecht bei Eintrag in gedruckte und elektronische Kundenverzeichnisse

Durch das Telekommunikationsgesetz hat der Kunde das Recht erhalten, selbst zu bestimmen, ob und in welcher Form er in ein öffentliches gedrucktes oder elektronisches Kundenverzeichnis (Telefonbuch) eingetragen wird (§ 89 Abs. 8 TKG, § 13 Abs. 2 TDSV). Die frühere Regelung des „Zwangseintrages“ ins Telefonbuch wurde zwar schon im Jahre 1991 aufgehoben, aber nach damaliger Rechtslage

konnte der Kunde sein Recht auf Nichteintrag nur durch Widerspruch wahrnehmen. Das Telekommunikationsgesetz und die Telekommunikations-Datenschutzverordnung legen demgegenüber eindeutig fest, dass der Telekommunikationsdiensteanbieter nur Einträge ins öffentliche Kundenverzeichnis aufnehmen darf, die vom Kunden ausdrücklich beantragt wurden. Anderenfalls darf ein Eintrag nicht erfolgen. Auch hat der Kunde jederzeit das Recht, seinen Eintrag ändern oder löschen zu lassen. Der Diensteanbieter hat den Kundenwunsch frühestmöglich umzusetzen.

Nach § 89 Abs. 8 TKG, § 13 Abs. 2 TDSV hat der Kunde darüber hinaus Ausgestaltungsrechte, denn er kann nicht nur entscheiden, ob und mit welchen Angaben wie Name, Anschrift, Beruf, Branche, Art des Anschlusses er überhaupt in öffentliche Verzeichnisse eingetragen werden möchte, sondern auch, ob die Eintragung nur in gedruckten oder in elektronischen öffentlichen Verzeichnissen oder in beiden erfolgen soll. Unterschiedliche Eintragungen in gedruckten oder elektronischen Verzeichnissen sind zwar möglich, ein separates Wahlrecht steht dem Kunden aber nicht zu.

Angaben über Mitbenutzer dürfen nur eingetragen werden, soweit diese sich damit einverstanden erklären (vgl. § 89 Abs. 8 Satz 3 TKG, § 13 Abs. 2 letzter Satz TDSV).

Bei einem Eintrag von Daten in öffentliche elektronische Kundenverzeichnisse sollte sich jeder Kunde darüber im Klaren sein, dass sein Telefonanschluss über Online-Dienste bekannt gegeben oder in ein CD-ROM-Verzeichnis eingetragen werden kann. Diese Daten können mit Hilfe eines PC gelesen und ausgewertet werden (siehe 5.4). Hierdurch können unter Umständen von einem PC-Nutzer kundenseitig nicht gewünschte oder unzulässige Datenverknüpfungen hergestellt werden, deren Zustandekommen vom Kunden oftmals nicht abzusehen ist.

Eintragungen von Kunden, die eine Eintragung in elektronische oder in gedruckte öffentliche Kundenverzeichnisse nicht wünschen, sind nach § 13 Abs. 2 Satz 3 TDSV in dem jeweils anderen Kundenverzeichnis zu kennzeichnen. Damit soll verhindert werden, dass z.B. der gewünschte Eintrag im gedruckten Kundenverzeichnis von einem CD-ROM-Produzenten automatisiert eingelesen („gescannt“) und in das elektronische Kundenverzeichnisse überführt wird.

Wegen dieser Kennzeichnung von Telefonbucheintragungen - z.B. durch einen * - haben sich viele Bürger an den Bundesbeauftragten für den Datenschutz gewandt: Diese befürchten eine „Stigmatisierung“ ihrer Person, etwa als technik- oder kommunikationsfeindlich. Deshalb wird als Alternative zur Kennzeichnung das

Konzept der Deutschen Telekom AG, durch einen allgemeinen Hinweis in den gedruckten oder elektronischen Verzeichnissen - an exponierter Stelle und mit deutlicher Texthervorhebung - darauf aufmerksam zu machen, dass in dem Verzeichnis auch Daten von Kunden enthalten sind, die mit einer Veröffentlichung in dem jeweils anderen Verzeichnis nicht einverstanden sind, vom Bundesbeauftragten für den Datenschutz begrüßt. Enthält ein Kundenverzeichnis nur einen allgemeinen Hinweis der vorbezeichneten Art, sind die Kunden in diesem Hinweis darauf aufmerksam zu machen, dass auf Wunsch auch eine Einzelkennzeichung ihrer Einträge vorgenommen wird.

Beachtet ein Anbieter den Wunsch des Betroffenen für Eintrag/Nichteintrag seines Telefonanschlusses nicht, verletzt er damit unwiderlegbar dessen schutzwürdige Interessen.

4.5.2.2 Wahlrecht in Bezug auf die Auskunftserteilung

Der Telekommunikationsdiensteanbieter darf nach § 89 Abs. 9 TKG, § 14 TDSV im Einzelfall Auskunft über die in öffentlichen Kundenverzeichnissen enthaltenen Rufnummern erteilen oder durch Dritte erteilen lassen (Telefonauskunft). Die Telefonauskunft über Rufnummern von Kunden 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 die auf Antrag des Kunden in öffentliche Kundenverzeichnisse aufgenommenen Angaben dürfen nur erteilt werden, wenn der Kunde mit einer weitergehenden Auskunftserteilung einverstanden ist. Widerspruch bzw. Einverständnis des Kunden sind in den Verzeichnissen des Diensteanbieters unverzüglich zu vermerken. Sie sind auch von den anderen Diensteanbietern zu beachten, sobald diese in zumutbarer Weise Kenntnis darüber erlangen konnten. Selbstverständlich kann der Kunde sein erteiltes Einverständnis jederzeit durch eine entsprechende Erklärung gegenüber dem Diensteanbieter zurückziehen; ebenso ist sein Widerspruch jederzeit möglich. Wenn ein im öffentlichen Kundenverzeichnis eingetragener Kunde der Auskunftserteilung widerspricht, so ist dies in den Auskunftsunterlagen des Unternehmens unverzüglich, in den gedruckten Verzeichnissen bei der nächsten Auflage, zu vermerken.

Die Übertragung der Auskunftserteilung an Dritte (Auskunftsdienste) ist nur zulässig, wenn der Diensteanbieter den Dritten verpflichtet, die Daten nur zur Auskunft zu verarbeiten und zu nutzen und dabei die Kundenwünsche zu beachten.

Nennt jemand, der eine Auskunft erhalten möchte, keinen Namen, sondern nur eine Telefonnummer, darf ihm nach § 14 Abs. 4 TDSV keine Auskunft über den Namen oder die Anschrift des Anschlussinhabers erteilt werden (Verbot der so genannten Inverssuche). Entsprechend dem dieser Vorschrift zugrundeliegenden Gedanken ist eine Inverssuche auch mittels „Telefonbuch-CD-ROM's", die eine Suche anhand von Telefonnummern ermöglichen, datenschutzrechtlich unzulässig (siehe 5.5).

4.5.2.3 Nutzung von Bestandsdaten zu Werbezwecken

Telekommunikations-Diensteanbieter dürfen nach § 89 Abs. 7 TKG die Bestandsdaten (siehe 4.5.1.2) ihrer Kunden für Zwecke der Werbung, Kundenberatung oder Marktforschung nutzen, soweit dies erforderlich ist und der Kunde eingewilligt hat. Dabei bezieht sich die Vorschrift lediglich auf die **Nutzung für eigene Zwecke**, also z.B. Werbung für den eigenen Diensteanbieter. Für die Übermittlung an andere Unternehmen, z.B. im Rahmen von Adressenhandel, ist nach § 3 Abs. 3 TDSV eine gesonderte Einwilligung des Kunden erforderlich, die den Vorschriften des Bundesdatenschutzgesetzes oder der Telekommunikations-Datenschutzverordnung entsprechen muss.

Sofern der Kunde in die Verwendung seiner Daten für Zwecke der (Eigen-)Werbung nicht eingewilligt oder einer solchen Verwendung widersprochen hat, ist die Weitergabe der Daten an Dritte zu Werbezwecken (Adressenhandel und -vermietung) auch dann unzulässig, wenn es sich um Daten handelt, die für die Veröffentlichung im öffentlichen Kundenverzeichnis vorgesehen oder bereits veröffentlicht sind.

Es ist allerdings jedem erlaubt, Daten aus öffentlichen Kundenverzeichnissen zu entnehmen und für Werbezwecke zu verwenden (§ 28 Abs. 1 Nr. 3 BDSG).

Die Deutsche Telekom AG gibt die für das gedruckte und elektronische Kundenverzeichnis vorgesehenen Daten ihrer Kunden an die

Deutsche Telekom Medien GmbH,
Postfach 16 02 11,
60065 Frankfurt/Main,
Telefon 069 / 2682-0,

weiter, wenn der Kunde eine Eintragung in das öffentliche Kundenverzeichnis beantragt oder in die Nutzung der eingetragenen Daten für Werbezwecke eingewilligt

hat. Kunden, die sich durch unverlangte Werbesendungen belästigt fühlen, können jederzeit die Löschung/Änderung der Eintragung ihres Telefonanschlusses in öffentlichen Kundenverzeichnissen verlangen (siehe 4.5.2.1) oder der Nutzung der eingetragenen Daten für Werbezwecke widersprechen; bei der Neuauflage des Kundenverzeichnisses dürfen ihre Daten dann nicht mehr bzw. nur geändert veröffentlicht werden.

Personen, die keine Werbung wünschen, können sich in verschiedene sogenannte **Robinson-Listen** aufnehmen lassen:

- Wer **keine Werbung per Post** wünscht, fordert ein Antragsformular unter folgender Anschrift an:

  Deutscher Direkt-Marketing-Verband
  - Robinson-Liste
  -Postfach 14 01
  71243 Ditzingen
  Telefon: 07156 / 95 10 10

- Wer **keine Werbung per Telefon wünscht,** kann seine Tel.-Nr. online eintragen lassen

  in die vom Interessenverband Deutsches Internet e. V. geführte Schutzliste http://www.telerobinson.de.

- Wer **keine Werbung per Fax** wünscht, ruft per Fax ein Antragsformular ab beim

  Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V. (BITKOM)
  unter der Telefax-Nummer: 01805/00 07 61
  (siehe auch 5.6.6)

- Wer **keine Werbung per E-Mail** wünscht, kann seine E-Mail-Adresse eintragen

  in die vom Interessenverband Deutsches Internet e.V. und des GSDI e.V. geführte Deutsche Mailschutzliste

  http://www.robinsonliste.de

- Wer **keine Werbung per SMS** wünscht, trägt seine Telefonnummer online in die vom

  Interessenverband Deutsches Internet e.V.
  geführte SMS-Schutzliste ein

  http://www.sms-robinson.de .

Der Vollständigkeit halber sei darauf hingewiesen, dass die Nutzung dieser Listen durch die Werbewirtschaft freiwillig ist. Ein Eintrag dort garantiert nicht, dass man absolut direktwerbefrei wird bzw. bleibt.

4.5.2.4 Einwilligung in die Datenübermittlung an die SCHUFA und an Wirtschaftsauskunfteien

Bonitätsprüfungen anhand von SCHUFA-Anfragen sind bei Firmen, die Geld- oder Warenkredite vergeben, seit langem üblich. Auch die Telekommunikations-Diensteanbieter - insbesondere die Mobilfunkanbieter - holen SCHUFA-Auskünfte ein, weil durch Nutzung eines Handys von der Freischaltung der Karte bis zur ersten Abrechnung bereits hohe Telefonrechnungen entstehen können. Ohne die Unterschrift unter die SCHUFA-Klausel wird man kaum ein Unternehmen zum Vertragsabschluss bewegen können, es sei denn, man ist zu einer ausreichend hohen Sicherheitsleistung bereit.

Eine gesonderte Unterschrift allein für die SCHUFA-Klausel ist im Antragsformular für Telekommunikationsdienstleistungen dann nicht erforderlich, wenn die Klausel in ihrem äußeren Erscheinungsbild hervorgehoben ist (§ 4a Abs. 1 Satz 4 BDSG), so dass die Aufmerksamkeit des (künftigen) Kunden gezielt auf die geforderte Einwilligung in die Verarbeitung der Daten gelenkt wird. Darüber hinaus sollte sich die Erklärung innerhalb des Antrages an exponierter Stelle befinden. Falls die Erklärung im Hauptteil des Antrages aus Platzgründen nur in verkürzter Form erscheint, muss sie einen deutlichen Hinweis auf den an anderer Stelle des Antrags abzudruckenden vollständigen Text enthalten. Der zwischen den Telekommunikations-Diensteanbietern und der SCHUFA vereinbarte Text der **SCHUFA-Klausel** ist als **Anhang 4** abgedruckt.

Auch für Anfragen an Wirtschaftsauskunfteien sind entsprechende Einwilligungserklärungen erforderlich.

4.5.2.5 Freiwillige Angaben in Verträgen über Telekommunikationsdienstleistungen

Telekommunikations-Diensteanbieter dürfen nach § 89 Abs. 10 Satz 1 TKG, § 3 Abs. 2 Satz 1 TDSV die Erbringung von Telekommunikationsdiensten - insbesondere also den Vertragsabschluss - nicht von der Angabe solcher personenbezogener Daten ihrer (künftigen) Kunden abhängig machen, die nicht für die Telekommunikationsdienstleistung selbst oder die Entgeltfestsetzung erforderlich sind (beispielsweise Angaben zur Religionszugehörigkeit oder zu einer Parteimitgliedschaft).

Entsprechendes gilt für die Einwilligung des Beteiligten (des Kunden) in die Verarbeitung und Nutzung der Daten für andere Zwecke (§ 3 Abs. 2 Satz 2 TDSV).

Aus datenschutzrechtlicher Sicht ist es erforderlich, Daten, die nur auf freiwilliger Basis abgefragt werden, als solche zu kennzeichnen. In den Antragsvordrucken einiger großer Firmen ist dies bereits der Fall.

4.5.2.6 Vorlage des Personalausweises oder Passes

Nach § 5 Abs. 4 TDSV ist der Telekommunikations-Diensteanbieter berechtigt, bei Vertragsabschluss oder dessen Änderung sowie im Zusammenhang mit dem Erbringen von Telekommunikationsdiensten die Vorlage eines amtlichen Ausweises zu verlangen. Er kann von dem Ausweis auch eine Kopie erstellen. Der Diensteanbieter darf dabei andere als die für Telekommunikationszwecke benötigten Daten nicht verarbeiten, d.h. nicht benötigte Daten müssen geschwärzt werden. Die Kopie ist vom Diensteanbieter unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Kunden zu vernichten.

In der Praxis hat diese Vorschrift vor allem für den Vertragsabschluss mit Mobilfunkunternehmen Bedeutung, da hier wegen der fehlenden Ortsbindung des Telefonanschlusses, d.h. Mobilität des Handys, die Feststellung der Identität und des gemeldeten Wohnsitzes der Kunden besonders wichtig ist.

4.5.3 Speicherung von Verbindungs- und Entgeltdaten zum Zwecke der Entgeltermittlung, der Entgeltabrechnung und des Entgeltnachweises

§ 7 Abs. 2 TDSV legt fest, dass folgende Daten für die Entgeltermittlung und Entgeltabrechnung verarbeitet werden dürfen:

- Verbindungsdaten,

- die Anschrift des Kunden 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,

- 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.

4.5.3.1 Speicherung der Verbindungsdaten

Die Speicherung der rechnungsrelevanten Verbindungsdaten richtet sich nach § 7 Abs. 3 TDSV. Hiernach hat der Telekommunikationsdiensteanbieter nach Beendigung der Verbindung (Telefonat oder sonstige Telekommunikation) aus den Verbindungsdaten (siehe 4.5.1.2) unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Nicht erforderliche Daten sind unverzüglich zu löschen. Hinsichtlich der Modalitäten der Speicherung hat der Kunde ein Wahlrecht:

- Grundsätzlich, d.h. wenn der Kunde keine besonderen Wünsche äußert, dürfen die Verbindungsdaten unter Kürzung der Zielnummer um die letzten drei Ziffern zu Beweiszwecken für die Richtigkeit der berechneten Entgelte höchstens sechs Monate nach Versendung der Rechnung gespeichert werden. Eine Ausnahme gilt für 0190er- oder 0900er-Mehrwertdienstruf nummern, die ungekürzt gespeichert werden dürfen. Hat der Kunde gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der vorgenannten Frist Einwendungen erhoben, dürfen die Verbindungsdaten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

- Abweichend davon hat auf Verlangen des Kunden der rechnungstellende Diensteanbieter grundsätzlich die bei ihm gespeicherten Verbindungsdaten

  1. vollständig, also ohne Kürzung der Zielnummer, zu speichern oder
  2. mit Versendung der Rechnung an den Kunden vollständig zu löschen. Dies hat allerdings zur Folge, dass der Diensteanbieter insoweit von der Pflicht zur Vorlage dieser Daten zum Beweis der Richtigkeit der Rechnung freigestellt ist.

Die Diensteanbieter gewähren oftmals bestimmte Formen der Gebührenbefreiung. Diese haben je nach Ausgestaltung hinsichtlich der Speicherung der Verbindungsdaten unterschiedliche Folgen, da die Befugnis zur Speicherung eng an die Erfordernisse der Entgeltberechnung geknüpft ist. Gewährt der Diensteanbieter an bestimmten Tagen oder in bestimmten Zeitintervallen eine Gebührenbefreiung, so haben die in dieser Zeit anfallenden Verbindungsdaten keinerlei Einfluss auf die Höhe der Rechnung. Folglich dürfen diese Verbindungsdaten auch nicht gespeichert werden und erscheinen demzufolge auch nicht im Einzelverbindungsnachweis. Gewährt der Diensteanbieter vertraglich jedoch zum Beispiel eine gewisse Anzahl von Freiminuten, so dürfen die diesbezüglichen Verbindungsdaten in der allgemein vom Kunden gewünschten Form gespeichert werden und erscheinen im ggf. vom Kunden verlangten Einzelverbindungsnachweis, weil der Kunde in der Lage sein muss nachzuvollziehen, dass er die vertraglich vereinbarten Freiminuten auch tatsächlich erhalten hat.

Besondere Sachverhalte (u.a. Entgeltpflicht für ankommende Verbindungen, geschlossene Benutzergruppen, Abrechnung zwischen Diensteanbietern, Einzug von Entgelten für Leistungen eines Dritten) sind in § 7 Abs. 3 Satz 2 und 3, § 7 Abs. 5 und § 7 Abs. 6 TDSV geregelt.

4.5.3.2 Speicherung von Entgeltdaten

Für die in § 7 Abs. 2 Nr. 2 und 3 TDSV genannten Entgeltdaten (siehe 4.5.1.2) sind keine besonderen Löschungsfristen festgelegt, d.h. die Speicherungsdauer z.B. für Zahlungsrückstände und Mahnungen hat sich am Grundsatz der Erforderlichkeit zu orientieren. Daraus folgt zwar nicht, dass solche Speicherungen sofort nach Begleichen ausstehender Zahlungen zu löschen sind; andererseits dürfen sie nach der Wiederaufnahme regelmäßiger Zahlungen jedoch nicht über einen angemessenen Zeitraum hinaus gespeichert bleiben.

4.5.4 Telefonrechnungen

Die Rechnungserstellung richtet sich nach den Allgemeinen Geschäftsbedingungen der einzelnen Anbieter von Telekommunikationsdiensten. Die Ausgestaltung der Rechnung und der Abrechnungszeitraum werden regelmäßig im Telekommunikationsvertrag festgelegt.

Wegen der Vielfalt der auf dem Telekommunikationsmarkt angebotenen Tarife, die oftmals erhebliche Preisunterschiede aufweisen, wird häufig nicht nur über den Anschlussnetzbetreiber, der den Zugang zum öffentlichen Telekommunikationsnetz zur Verfügung stellt, sondern im so genannten Call-by-Call-Verfahren auch über andere Diensteanbieter (Verbindungsnetzbetreiber) telefoniert. Aus diesem Grund hat der Verordnungsgeber aus Gründen des Verbraucherschutzes den Anschlussnetzbetreiber zur Erstellung einer **Gesamtrechnung** mit den Entgelten aller in Anspruch genommenen Diensteanbieter verpflichtet. § 15 TKV schreibt für die Rechnungslegung vor, dass der Diensteanbieter, der dem Kunden den Zugang zum öffentlichen Telekommunikationsnetz zur Verfügung stellt, eine Rechnung zu erstellen hat, die auch die Entgelte für Verbindungen ausweist, die durch Auswahl anderer Anbieter von Netzdienstleistungen über den Netzzugang des Kunden entstehen. Die Rechnung muss die einzelnen Anbieter und zumindest die Gesamthöhe der auf sie entfallenen Rechnungsbeträge erkennen lassen. Die Möglichkeit, mit den Verbindungsnetzbetreibern eine hiervon abweichende Regelung, beispielsweise bei Call-by-Call mit Anmeldung oder bei Preselection, die eigene Rechnungserstellung zu vereinbaren, bleibt unberührt.

Für den Kunden ist es auch von großem Nutzen, wenn er seine Rechnung nicht nur in der üblichen pauschalierten Form erhält, sondern wenn die Gespräche in einer detaillierten Einzelaufstellung aufgelistet sind. Er hat damit die Möglichkeit, die entstandenen Entgeltforderungen zu überprüfen und zu kontrollieren. Nach § 14 TKV kann er von seinem Diensteanbieter unentgeltlich einen solchen **Einzelverbindungsnachweis (EVN)** verlangen. Die Erteilung eines EVN ist nur nach Maßgabe der nachstehend unter 4.5.4.1 erläuterten Vorschriften der Telekommunikations-Datenschutzverordnung zulässig.

Die Weiterentwicklung der Informationstechnik und die ständig anwachsende Zahl der Internetnutzer hat Telekommunikationsdiensteanbieter bereits veranlasst, eine neue Form der Rechnungserstellung anzubieten: die **„Rechnung Online**“ (siehe 4.5.4.2).

Seit Anfang 2001 kann der Kunde gemäß § 18 TKV gegenüber seinem Diensteanbieter vorgeben, bis zu welcher Entgelthöhe er die Dienstleistungen in Anspruch nehmen will. Die Regulierungsbehörde für Telekommunikation und Post hat hierzu mehrere Umsetzungsmöglichkeiten in ihrer Amtsblattmitteilung vom 20.12.2000 festgelegt, die im Internet unter www.regtp.de abrufbar ist.

4.5.4.1 Einzelverbindungsnachweis

Es ist ein berechtigtes Kundeninteresse, nach Erhalt der Telefonrechnung nicht nur die rechnerische Richtigkeit der Entgelte überprüfen zu können, sondern auch in der Lage zu sein, die Entstehung der einzelnen Kosten zu kontrollieren. Diesem Verbraucherschutzgedanken wird durch § 14 TKV Rechnung getragen, wonach der Diensteanbieter auf Verlangen des Kunden im Rahmen der technischen Möglichkeiten und der datenschutzrechtlichen Vorschriften eine nach Einzelverbindungen aufgeschlüsselte Rechnung (Einzelverbindungsnachweis, EVN) zu erteilen hat. Die datenschutzrechtliche Grundlage für die Erteilung des EVN bildet § 89 Abs. 2 Nr. 3 Buchstabe a) TKG, die einzelnen Voraussetzungen sind darüber hinaus in § 8 TDSV geregelt.

Nach § 14 TKV muss die Standardform des EVN unentgeltlich erteilt werden. Zu der Frage, welche Voraussetzungen ein **Standardeinzelverbindungsnachweis** erfüllen muss, hat die Regulierungsbehörde für Telekommunikation und Post ihre Auffassung mit Mitteilung Nr. 309/1999 im Amtsblatt Nr. 13/1999 bekannt gegeben. Gleichzeitig hat sie zur Information der Öffentlichkeit eine sogenannte Positivliste erstellt, in denen die Diensteanbieter aufgeführt sind, die sich an die aus dem Telekommunikationsgesetz, der Telekommunikations-Datenschutzverordnung und der Telekommunikations-Kundenschutzverordnung resultierenden Vorgaben zum Standard-EVN halten. Die Aufnahme in die Positivliste erfolgt auf freiwilliger Basis. Die Liste soll bis auf Weiteres halbjährlich aktualisiert und im Amtsblatt der Regulierungsbehörde veröffentlicht werden. Sie steht auch der Allgemeinheit im Internet unter www.regtp.de zur Verfügung. Zu den notwendigen Angaben im Standard-EVN gehören:

- das Datum der Gespräche,
- die Anschlussnummer des Kunden,
- je nach Wunsch des Kunden gekürzte oder vollständige Zielrufnummern,
- zwei der Merkmale Beginn und Ende oder Dauer der Verbindung sowie
- eines der Merkmale Tarifeinheit oder Entgelt für das Einzelgespräch.

Die **Voraussetzungen** für die Erteilung eines EVN sind abschließend in § 8 TDSV geregelt:

1. Der Kunde muss den EVN vor dem maßgeblichen Abrechnungszeitraum schriftlich beantragt haben.

2. Bei Anschlüssen im Privathaushalt muss der Kunde schriftlich erklärt haben, dass er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber informiert hat und künftige Mitbenutzer unverzüglich über die Mitteilung der Verbindungsdaten an ihn informieren wird.

3. Bei Anschlüssen in Betrieben und Behörden muss der Kunde schriftlich erklärt haben, dass die Mitarbeiter informiert worden sind, künftige Mitarbeiter informiert werden und der Betriebsrat bzw. der Personalrat entsprechend den gesetzlichen Vorschriften beteiligt worden oder eine solche Beteiligung nicht erforderlich ist. Dieser Mitbenutzerschutz gilt auch in den Fällen, in denen ein Arbeitgeber seinen im Außendienst beschäftigten Mitarbeitern Firmenhandies zur Verfügung stellt. Eine Zustimmung der Arbeitnehmer ist - unabhängig davon, ob nur geschäftliche oder auch private Nutzung des Anschlusses zugelassen ist - nicht erforderlich.

Die Zielrufnummern der einzelnen Verbindungen können im EVN sowohl vollständig als auch um die letzten drei Ziffern gekürzt dargestellt werden. Dies richtet sich danach, welche Wahl der Kunde hinsichtlich der Speicherung der Verbindungsdaten (siehe 4.5.3.1) getroffen hat. Eine ungekürzte Wiedergabe im EVN ist nur möglich, wenn er gemäß § 7 Abs. 4 Nr. 1 TDSV die vollständige Speicherung der Verbindungsdaten nach Rechnungsversand verlangt hat.

Nach dem Wortlaut des § 8 Abs. 1 TDSV sind im EVN nur die Verbindungen mitzuteilen, für die der Kunde entgeltpflichtig ist. Auch wenn dies den Schluss zulässt, dass **entgeltfreie Verbindungen** generell nicht im EVN aufgeführt werden dürfen, muss diese Frage jedoch differenziert betrachtet werden. Bei einem echten Flatrate-Tarif, bei dem das gesamte Gebührenaufkommen in festgelegten Zeiträumen oder an bestimmten Tagen (z.B. an Wochenenden, sonn- und feiertags) durch den vereinbarten Pauschalbetrag abgegolten ist, ist die Sachlage klar. Die Verbindungsdaten werden für die Berechnung des Entgelts nicht benötigt und sind nach § 7 Abs. 3 TDSV nach Beendigung der Verbindung unverzüglich zu löschen. Sie dürfen daher auch nicht im EVN aufgeführt werden. Gleiches gilt sicherlich auch für entgeltfreie Verbindungen zu 0800-er Rufnummern, bei denen der Angerufene die Kosten übernimmt. Anders sieht es dagegen bei Tarifen aus, die einen Freibetrag für

eine bestimmte Anzahl von Gebühreneinheiten vorsehen. Da die über den pauschalen Freibetrag hinausgehenden Gespräche entgeltpflichtig sind, sind auch die bis dahin zustande gekommenen Verbindungen entgeltrelevant und für die Nachprüfung der Rechnung erforderlich. Gegen eine Auflistung im EVN bestehen daher keine Bedenken.

Telefonate zu Anschlüssen von Personen, Behörden oder Organisationen, die der anonymen Beratung im sozialen oder kirchlichen Bereich dienen, darf der EVN nicht erkennen lassen (vgl. § 89 Abs. 2 Nr. 3 a TKG i.V.m. § 8 Abs. 2 TDSV). 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 der Gesundheitsberatung.

Das Verfahren, wie derartige Beratungsstellen anerkannt werden, ist in der Telekommunikations-Datenschutzverordnung geregelt. Voraussetzung hierfür ist, dass die jeweilige Beratungsstelle in eine zentrale und von der Regulierungsbehörde für Telekommunikation und Post geführte Liste aufgenommen wird. Dies erfolgt, wenn die betroffene Beratungsstelle durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts ihre Tätigkeit nachgewiesen hat. Diese Liste wird von der Regulierungsbehörde zum Abruf durch die Telekommunikationsdiensteanbieter im automatisierten Verfahren bereitgestellt. Die Diensteanbieter sind verpflichtet, den Inhalt der Liste quartalsweise abzufragen und bei ihrem Abrechnungsverfahren zu berücksichtigen.

Wie der Schutzzweck der Regelung konkret umgesetzt und erreicht werden kann, dass die Verbindung im EVN nicht erkennbar ist, ist in der TDSV nicht festgelegt worden. In der amtlichen Begründung hat der Verordnungsgeber jedoch ausgeführt, dass Name und die Zielnummer der Beratungsstelle sowie die Dauer der Verbindung nicht im EVN erscheinen sollten. Eine Verkürzung der Rufnummer um die letzten drei Ziffern gewährleistet die anonyme Kommunikation nicht. Die Vertraulichkeit kann nur dadurch gewahrt werden, dass sich die Angaben im EVN auf das Datum, die Uhrzeit und die Kosten der Verbindung beschränken. Sinnvoll ist sicherlich eine Summenzeile, die eine anonyme Aufaddierung aller Anrufe zu Beratungsstellen enthält. Soweit der Anruf zu einer Beratungsstelle entgeltfrei ist (wie z.B. derzeit Anrufe bei der Telefonseelsorge), darf er natürlich überhaupt nicht im EVN erscheinen.

4.5.4.2 „Rechnung Online“

Neuerdings wird von Telekommunikationsdiensteanbietern auch der Service „Rechnung Online“ angeboten. Er ermöglicht dem Kunden, die Daten seiner Rechnung über das Internet mit einem aktuellen Web-Browser online anzusehen und auf seinen PC herunterzuladen. Anschließend kann er die Daten nach Belieben mit dem eigenen PC be- und verarbeiten. Zum Teil wird mit „Rechnung Online“ bereits selbst eine ganze Reihe von Analysemöglichkeiten im direkten Zugriff zur Verfügung gestellt.

Aus datenschutzrechtlicher Sicht bestehen gegen den Service „Rechnung Online“ keine Bedenken, wenn hierbei bestimmte, sich aus der Telekommunikations-Datenschutzverordnung ergebende Anforderungen erfüllt sind:

Da in der Regel ein großer Teil der Funktionalitäten auf einer Verarbeitung der Verbindungsdaten basiert und zugleich eine Einsichtnahme in den Einzelverbindungsnachweis online möglich ist, hält der Bundesbeauftragte für den Datenschutz es für erforderlich, dass der Kunde zuvor einen Einzelverbindungsnachweis (siehe 4.5.4.1) beantragt und nicht die vollständige Löschung der Verbindungsdaten mit Versendung der Rechnung nach § 7 Abs. 4 Nr. 2 TDSV (siehe 4.5.3.1) verlangt hat. Weil mit „Rechnung Online“ das Kommunikationsverhalten einzelner Familienmitglieder oder Firmenmitarbeiter differenzierter analysiert werden kann als bei einem rein chronologisch aufgebauten Einzelverbindungsnachweis, hält es der Bundesbeauftragte für den Datenschutz zudem für geboten, den Kunden aufzufordern, Familienmitglieder bzw. Firmenangehörige hierüber zu informieren.

Wenn unter bestimmten Voraussetzungen bei „Rechnung Online“ nicht auf einzelne Verbindungsdaten abgestellt wird, beispielsweise bei Rechnungen, die am betriebswirtschaftlichen Bedarf von Unternehmen mit umfangreichem Telekommunikationsaufkommen orientiert sind und lediglich Entgeltdaten enthalten, ist die Beantragung eines Einzelverbindungsnachweises und die Speicherung der Verbindungsdaten über den Zeitpunkt des Rechnungsversands hinaus nicht zwingend erforderlich.

4.5.4.3 Rechnungserstellung im Ausland

Aufgrund der vielfältigen Verflechtungen der in Deutschland tätigen Telekommunikationsdiensteanbieter mit ausländischen Telekommunikationsunternehmen wird aus Wirtschaftlichkeitsgründen vermehrt auf

das Know how des ausländischen Partnerunternehmens sowie auf dort vorhandene Software- oder Hardwareressourcen zurückgegriffen. Beispiele sind u.a. Programme zur Aufbereitung der bei einem Telefonat entstehenden Verbindungsdaten für die Rechnungserstellung sowie Programme zur Erstellung und zum Druck von Kundenrechnungen. Auch der Briefversand der Rechnungen an die deutschen Kunden ist aus dem Ausland oft billiger. Das setzt die Übermittlung von Verbindungsdaten an die ausländische Stelle voraus.

Eine spezielle Regelung für die Weitergabe von personenbezogenen Daten im Bereich der Telekommunikation an ausländische Stellen gab es lange Zeit nicht. Die Telekommunikations-Datenschutzverordnung hat hierfür eine Regelung in § 3 Abs. 6 getroffen. Danach ist die Übermittlung personenbezogener Daten an ausländische Stellen zulässig, soweit es für die Erbringung von Telekommunikationsdiensten, für die Erstellung oder Versendung von Rechnungen oder für die Bekämpfung des Missbrauchs von Telekommunikationsdiensten erforderlich ist. Dabei sieht der Verordnungsgeber es schon als ausreichend an, wenn z.B. die Erstellung der Rechnung im Ausland kostengünstiger ist.

Für die Kunden bedeutet dies, dass auch ohne ihre Einwilligung eine Datenübermittlung an ausländische Stellen in diesem begrenzten Umfang erlaubt ist.

Die Übermittlung von Daten in das Ausland muss zudem gemäß § 3 Abs. 6 TDSV nach Maßgabe der Vorschriften des BDSG zulässig sein. Einschlägig ist hierfür der seit dem 23.05.2001 geltende § 4b BDSG, der durch das Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze vom 22.05.2001 (siehe Anhang 1 I.2) in das BDSG neu eingefügt wurde. Der Gesetzgeber hat in § 4b Abs. 1 BDSG eine Privilegierung für eine Übermittlung der Daten in die Mitgliedstaaten der Europäischen Union vorgesehen und die entsprechenden Vorschriften des BDSG für anwendbar erklärt. Für eine Übermittlung der Daten an Stellen außerhalb der Union wird nach § 4b Abs. 2 BDSG auf die Angemessenheit des Datenschutzniveaus in dem entsprechenden Land abgestellt. Die Kriterien zur Bestimmung des abgemessenen Datenschutzniveaus sind in § 4b Abs. 3 BDSG geregelt und wurden dem Artikel 25 der europäischen Datenschutzrichtlinie 95/46/EG entnommen.

Der Bundesbeauftragte für den Datenschutz empfiehlt den Telekommunikationsdiensteanbietern, ihre Kunden über eine Datenverarbeitung im Ausland im Rahmen des Vertragsabschlusses zu informieren und für den Fall, dass die Daten ins Ausland auf elektronischem Wege übertragen werden sollen, dies in

verschlüsselter Form durchzuführen, da die Verbindungsdaten dem besonderen Schutz des Fernmeldegeheimnisses nach § 85 TKG unterliegen.

4.5.4.4 Rechnungseinwendungen

Soweit der Anschlussinhaber auf seinen Antrag mit der Telefonrechnung einen Einzelverbindungsnachweis (siehe 4.5.4.1) erhält, kann er die Höhe der Rechnung an Hand der aufgeschlüsselten Verbindungsdaten ohne weiteres überprüfen. Anders sieht es aus, wenn lediglich eine pauschalierte Rechnung erstellt wird und Zweifel an der Höhe der geforderten Verbindungsentgelte bestehen. Der Telekommunikationsdiensteanbieter muss in diesem Fall die geltend gemachte Forderung näher begründen und die Rechnung detaillieren.

In § 16 TKV ist deshalb geregelt, dass das Verbindungsaufkommen unter Wahrung des Schutzes der Mitbenutzer auch ohne Auftrag zur Erteilung eines Einzelverbindungsnachweises nach den einzelnen Verbindungsdaten aufzuschlüsseln ist, wenn ein Kunde Einwendungen gegen die Höhe der ihm in Rechnung gestellten Verbindungsentgelte erhebt.
Die datenschutzrechtliche Grundlage für die Mitteilung der gespeicherten Einzelverbindungsdaten an den Kunden zwecks Überprüfung der Rechnung ist in § 8 Abs. 1 Satz 5 TDSV enthalten. Allerdings mit der Einschränkung, dass die Zielrufnummern nur unter Kürzung der letzten drei Ziffern mitgeteilt werden dürfen. Der Kunde hat keinen Anspruch auf Mitteilung der vollständigen Zielrufnummern Eine Ausnahme gilt nur für die 0190er- oder 0900er-Mehrwertdienstrufnummern, die grundsätzlich ungekürzt gespeichert und mitgeteilt werden dürfen. Anders als beim vor Versendung der Rechnung beauftragten Einzelverbindungsnachweis ist hierbei nicht vorgeschrieben, dass der Anschlussinhaber zur Information der Mitbenutzer des Anschlusses verpflichtet ist und eine entsprechende Erklärung abgeben muss.

Im Falle von Einwendungen gegen die Rechnung dürfen im übrigen die Verbindungsdaten beim Diensteanbieter ungeachtet der Höchstspeicherfrist von sechs Monaten nach Rechnungsversand (siehe 4.5.3.1) solange gespeichert werden, bis die Einwendungen abschließend geklärt sind (§ 7 Abs. 3 Satz 5 TDSV).

Hat der Kunde allerdings von seiner Möglichkeit Gebrauch gemacht, die vollständige Löschung der Verbindungsdaten mit Rechnungsversand zu verlangen (siehe 4.5.3.1), ist der Diensteanbieter insoweit gemäß § 16 Abs. 2 TKV von der Pflicht zur Vorlage dieser Daten zum Beweis der Richtigkeit der Rechnung freigestellt.

4.5.4.5 Übermittlung von Verbindungs- und Entgeltdaten an Dritte

Nach § 15 TKV ist dem Kunden von seinem Anschlussnetzbetreiber grundsätzlich eine Rechnung zu erstellen, die auch die Entgelte für die in Anspruch genommen anderen Verbindungsnetzbetreiber (z.B. Call-by-Call-Anbieter) ausweist. Dies setzt zwingend die Übermittlung von Verbindungsdaten zum Zwecke der Entgeltermittlung und Entgeltberechnung voraus. Die Erlaubnis hierzu ergibt sich aus § 7 Abs. 1 Satz 1 TDSV. Danach dürfen Diensteanbieter einander die Verbindungsdaten übermitteln und nutzen, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Kunden benötigt werden.

Nach § 7 Abs. 1 Satz 2 und 3 TDSV dürfen darüber hinaus Bestands- und Verbindungsdaten auch an Dritte übermittelt werden, wenn zwischen Diensteanbieter und Drittem ein Vertrag über den Einzug des Entgelts besteht (z.B. mit einem Inkassounternehmen) und die Übermittlung für den Einzug des Entgelts und die Erstellung einer detailliierten Rechnung erforderlich ist. Voraussetzung ist auch, dass der Dritte vertraglich zur Einhaltung des Fernmeldegeheimnisses sowie der einschlägigen datenschutzrechtlichen Bestimmungen der Telekommunikations-Datenschutzverordnung verpflichtet worden ist. Eine Einwilligung des Kunden in die Datenübermittlung ist nicht erforderlich. Die Regelung begründet für den Diensteanbieter kein eigenständiges Recht, die Forderung an das Inkassounternehmen mit der Folge abzutreten, dass dieses die Forderung gegenüber dem Kunden unmittelbar als eigene Forderung geltend machen kann.

4.5.5 Qualitäts- und Missbrauchskontrolle

4.5.5.1 Einzelfallkontrollen und -auswertungen

Gemäß § 89 Abs. 2 Nr. 1d und e TKG i.V.m. § 9 TDSV ist es zulässig, für das Erkennen und Beseitigen von Störungen sowie das Aufklären und Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen von Telekommunikationsnetzen und -dienstleistungen Bestands- und Verbindungsdaten zu erheben, zu verarbeiten und zu nutzen. Obwohl die beiden Vorschriften die Entgeltdaten (siehe 4.5.1.2) nicht ausdrücklich aufführen, dürfen auch diese Daten verwendet werden, um Leistungserschleichungen aufzuklären und zu unterbinden. Dies dient letztlich der korrekten Abrechnung und wird somit von der Zweckbestimmung dieser Daten umfasst.

Für den Fall der Leistungserschleichung bzw. der rechtswidrigen Inanspruchnahme müssen allerdings tatsächliche Anhaltspunkte vorliegen, die schriftlich zu dokumentieren sind. Ein solcher Anhaltspunkt ist insbesondere gegeben, wenn ein begründeter Kundenantrag oder eine Kundenbeschwerde vorliegt. Eine „vorsorgliche Speicherung für den Fall, dass ...“ ist unzulässig.

Es dürfen sämtliche zum Zeitpunkt der Überprüfung zulässigerweise gespeicherten Daten ausgewertet werden (siehe 4.5.3).

4.5.5.2 Auswertung des Gesamtbestandes aller Verbindungsdaten

Darüber hinaus dürfen die Diensteanbieter nach § 9 Abs. 2 TDSV die erhobenen Verbindungsdaten in der Weise verarbeiten und nutzen, dass aus dem Gesamtbestand aller Verbindungsdaten (sie dürfen maximal 6 Monate nach Rechnungsversand gespeichert werden), die Daten derjenigen Verbindungen ermittelt werden, für die tatsächliche Anhaltspunkte einer rechtswidrigen Inanspruchnahme von Telekommunikationsnetzen und -diensten vorliegen. Hier dürfen also nicht nur die Daten der Kunden einbezogen werden, bei denen tatsächliche Anhaltspunkte für eine missbräuchliche Inanspruchnahme bestehen, sondern die aller Kunden. Darüber hinaus darf der Diensteanbieter aus den erhobenen Verbindungsdaten und den Bestandsdaten einen Gesamtdatenbestand bilden, der in pseudonymisierter Form Aufschluss über die von den einzelnen Kunden erzielten Umsätze gibt und unter Zugrundelegung geeigneter Missbrauchskriterien das Auffinden solcher Verbindungen ermöglicht, bei denen der Verdacht einer Leistungserschleichung besteht. Dabei sind die Daten der anderen Verbindungen unverzüglich zu löschen.

Über die Einführung und Änderung dieser Verfahren sind die Regulierungsbehörde für Telekommunikation und Post und der Bundesbeauftragte für den Datenschutz in Kenntnis zu setzen.

4.5.5.3 Aufschalten auf bestehende Verbindungen

Zum Erkennen und Eingrenzen von Störungen sowie zur Durchführung von Umschaltungen ist nach § 89 Abs. 5 TKG das Aufschalten auf bestehende Verbindungen (das umfasst auch das Mithören des Gespräches) erlaubt, soweit dies betrieblich erforderlich ist. Das Aufschalten muss den betroffenen

Gesprächsteilnehmern allerdings durch ein akustisches Signal angezeigt und ausdrücklich mitgeteilt werden.

Zur Missbrauchsbekämpfung ist das Aufschalten (also insbesondere auch das Mithören) nicht erlaubt.

Diese Vorschrift richtet sich nicht nur an die Betreiber öffentlicher Kommunikationsnetze sowie Diensteanbieter, die ihr Angebot der Öffentlichkeit zur Verfügung stellen, sondern an alle, die geschäftsmäßig Telekommunikationsdienste erbringen (siehe 4.5.1.2). Somit gilt diese Vorschrift z. B. auch für Nebenstellenanlagen von Behörden und Betrieben sowie für Hotels, Krankenhäuser und ähnliche Einrichtungen, soweit dort die Nutzung der TK-Anlage auch für Privatgespräche gestattet ist.

Das Aufschalten auf laufende Gespräche berührt das grundrechtlich geschützte Fernmeldegeheimnis (siehe 4.2). Der Vertraulichkeit des nicht öffentlich gesprochenen Wortes kommt aus verfassungsrechtlicher Sicht große Bedeutung zu. Der Bürger muss im Regelfall davon ausgehen können, dass ein Gespräch, das er mit einem anderen führt, nicht heimlich belauscht oder aufgezeichnet wird. Da die Benutzung des Telefons, z. B. im beruflichen Bereich, fester Bestandteil des Alltags ist, muss dies auch für die genannten Nebenstellenanlagen gelten. Die Technik der modernen Telekommunikationsanlagen schafft hier doch Gefährdungen, die erkannt und begrenzt werden müssen. Der Bundesbeauftragte für den Datenschutz hält es für erforderlich, dass nicht nur ein Abschalten des deutlich hörbaren Hinweistones technisch ausgeschlossen sein sollte, sondern auch dessen Lautstärke sollte unveränderbar sein, damit das Aufschalten nicht unbemerkt bleiben kann.

4.5.5.4 Behandlung von Nachrichteninhalten

Nach § 89 Abs. 3 TKG dürfen nur die näheren Umstände der Telekommunikation für Zwecke der Qualitäts- und Missbrauchskontrolle erhoben, verarbeitet und genutzt werden, also nicht die Nachrichteninhalte.

Nachrichteninhalte dürfen nach § 89 Abs. 4 TKG (ausnahmsweise) aufgezeichnet, Dritten zugänglich gemacht oder sonst verarbeitet werden, soweit dies Bestandteil eines von dem Kunden in Anspruch genommenen Telekommunikationsdienstes ist. So dürfen z.B. im Rahmen eines Voice-Box-Dienstes Nachrichten aufgezeichnet und für den Abruf bereit gehalten werden.

4.5.5.5 Steuersignale

Speziell zur Missbrauchsbekämpfung ist nach § 89 Abs. 3 TKG und § 9 Abs. 4 TDSV im Einzelfall die Erhebung, Verarbeitung und Nutzung von Steuersignalen erlaubt, soweit dies unerlässlich ist. Steuersignale werden durch maschinelles „Abtasten“ elektronisch übermittelter Kommunikation erhoben, ohne dass dabei der Nachrichteninhalt zur Kenntnis genommen wird.

4.5.6 Bedrohende oder belästigende Anrufe – Einrichtung von Fangschaltungen

Erhält ein Kunde bedrohende oder belästigende Anrufe und trägt er dies seinem Telekommunikations-Diensteanbieter in einem zu dokumentierenden Verfahren schlüssig vor, so hat der Diensteanbieter nach § 89 Abs. 2 Nr. 3 b TKG in Verbindung mit § 10 TDSV auf schriftlichen Antrag - auch netzübergreifend - Auskunft über die Anschlüsse zu erteilen, von denen die Anrufe ausgehen. Hierzu wird bei dem bedrohten oder belästigten Kunden eine sog. Fangschaltung eingerichtet, mit deren Hilfe der Kunde die betreffenden Anrufe kennzeichnen kann. Die Auskunft darf sich nur auf Anrufe beziehen, die nach dem Antrag durchgeführt werden. Der Diensteanbieter darf grundsätzlich die Nummern, Namen und Anschriften der Inhaber dieser Anschlüsse sowie Datum und Uhrzeit des Beginns der Verbindungen und Verbindungsversuche erheben, speichern und seinem Kunden mitteilen. Dies gilt allerdings nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten (z.B. innerhalb einer Firma). Sind die Inhaber der gefangenen Anschlüsse nicht in einem öffentlichen Kundenverzeichnis eingetragen, dürfen dem Kunden jedoch **lediglich** Namen und Anschriften der Anschlussinhaber mitgeteilt werden.

Für die Einrichtung einer Fangschaltung müssen tatsächliche Anhaltspunkte vorgetragen werden, aus denen sich – aus der Sicht des Betroffenen – eine Bedrohung oder Belästigung ergibt. So sind beispielsweise detaillierte Angaben zur Häufigkeit und Art dieser Anrufe zu machen. Nicht ausreichend ist also die alleinige Behauptung, telefonisch bedroht oder belästigt worden zu sein. Die Notwendigkeit der Spezifizierung der Bedrohungen oder Belästigungen und die Schlüssigkeit der Darlegung durch den Antragsteller hat ihren Grund darin, dass das Grundrecht auf Unverletzlichkeit des Fernmeldegeheimnisses (Art. 10 Grundgesetz) für jedermann und damit auch für den vermeintlich belästigenden bzw. bedrohenden

Telekommunikationsteilnehmer gilt. Nur bei begründetem Verdacht auf eine unzulässige Handlung darf in das Fernmeldegeheimnis eingegriffen werden.

Der Diensteanbieter hat daher die Angaben des Antragstellers sorgfältig zu prüfen, er ist allerdings weder in der Lage noch verpflichtet – wie beispielsweise ein Gericht – zu überprüfen, ob die Äußerungen des Antragstellers auch objektiv der Wahrheit entsprechen. Ferner macht sich der Diensteanbieter die Darlegung des Antragstellers auch nicht zu eigen, wenn er entsprechend der gesetzlichen Verpflichtung auf Grund des Antrages eine Fangschaltung einrichtet. In diesem Zusammenhang ist jedoch zu beachten, dass der Missbrauch der Überwachungsmöglichkeit durch den antragstellenden Kunden strafbar ist (§§ 43 Abs. 2 Nr. 3, 44 Abs. 1 BDSG).

Zur Missbrauchsvermeidung muss ferner eine weitere Schlüssigkeitsprüfung durchgeführt werden, bevor der Diensteanbieter dem Antragsteller den „gefangenen“ Anschluss bekannt geben darf. Hierzu ist es mindestens erforderlich, dass der Antragsteller die belästigenden oder bedrohenden Anrufe nach Datum, Uhrzeit oder anderen geeigneten Kriterien eingrenzt, soweit ein Missbrauch nicht auf andere Weise ausgeschlossen werden kann. Sollten sich aufgrund der Daten des „gefangenen“ Anschlusses Informationen oder Anhaltspunkte ergeben, die den Vortrag des Antragstellers nicht mehr schlüssig erscheinen lassen (z.B. wenn es sich bei der „gefangenen“ Rufnummer um die einer Person des öffentlichen Interesses, einer dem Zeugenschutzprogramm unterliegenden Person oder einer besonders schützenswerten Einrichtung handelt), empfiehlt der Bundesbeauftragte für den Datenschutz aus Datenschutzgesichtspunkten nachdrücklich, die Information dem Antragsteller nicht bekannt zu geben. Hat der Diensteanbieter Anhaltspunkte für einen Missbrauch der Überwachungsmöglichkeit, so darf er keine Auskunft erteilen.

Um dem Inhaber des „gefangenen“ Anschlusses die Möglichkeit zu geben, die rechtliche Zulässigkeit einer gegen ihn gerichteten Fangschaltung im Nachhinein überprüfen zu lassen, ist dieser anschließend davon zu unterrichten. Das Bundesverfassungsgericht hat in seinem sog. Fangschaltungsbeschluss von 1992 (siehe Anhang 2) ausdrücklich auf die Zulässigkeit eines solchen Verfahrens hingewiesen. Von der Unterrichtung kann jedoch abgesehen werden, wenn der Antragsteller in schriftlicher Form schlüssig vorgetragen hat, dass ihm aus dieser Mitteilung wesentliche Nachteile entstehen können und diese Nachteile bei Abwägung mit den schutzwürdigen Interessen des Anrufers als wesentlich schwerwiegender erscheinen. Erhält allerdings der Kunde, 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.

Im Falle einer netzübergreifenden Anschlussermittlung sind die an der Verbindung mitwirkenden anderen Diensteanbieter verpflichtet, dem Diensteanbieter des bedrohten oder belästigten Kunden die erforderlichen Auskünfte zu erteilen, sofern sie über diese Daten verfügen.

Gefangen werden können auch Anrufe, bei denen der Angerufene den Hörer noch nicht aufgenommen hat. Im Rahmen der Verbindungsdatenerfassung werden solche Verbindungsversuche – da sie nicht entgeltpflichtig sind – jedoch nicht registriert und erscheinen demzufolge nicht im Einzelverbindungsnachweis (EVN). Zur Vermeidung von Missverständnissen ist es für den Diensteanbieter geboten, bei der Mitteilung an den Antragsteller die Verbindungsdaten derart zu kennzeichnen, dass für ihn und auch für den Benachrichtigten erkennbar wird, ob es sich um Verbindungen oder Verbindungsversuche gehandelt hat.

Aus Gründen der Datensicherheit und des Datenschutzes haben die Diensteanbieter die Regulierungsbehörde für Telekommunikation und Post sowie den Bundesbeauftragten für den Datenschutz über die Einführung und Änderung des Verfahrens zur Einrichtung von Fangschaltungen unverzüglich in Kenntnis zu setzen.

4.5.7 Rufnummernanzeige/Rufnummernunterdrückung

4.5.7.1 Wahlmöglichkeiten

§ 11 TDSV regelt, dass Diensteanbieter, die die Anzeige der Rufnummer auf dem Display des TK-Endgerätes anbieten, ihren Kunden folgende Wahlmöglichkeiten einräumen müssen, soweit dies technisch möglich ist:

- Für eingehende Anrufe kann die Anzeige der Nummer auf dem Display des Angerufenen dauernd oder im Einzelfall unterdrückt werden.

- Bei abgehenden Anrufen kann die Anzeige der Rufnummer auf dem Display des Angerufenen dauernd oder im Einzelfall unterdrückt werden.

- Ferner besteht die Möglichkeit, eingehende Anrufe abzuweisen, wenn vom Anrufenden die Rufnummernanzeige unterdrückt wurde.

Gemäß § 11 Abs. 2 TDSV 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 des Kunden in dem öffentlichen Kundenverzeichnis seines Diensteanbieters entsprechend zu kennzeichnen.

Ist ein Kunde nicht in ein öffentliches Kundenverzeichnis eingetragen, muss nach § 11 Abs. 3 TDSV die Anzeige seiner Rufnummer grundsätzlich unterbleiben. Der Kunde kann allerdings ausdrücklich bestimmen, dass auch ohne eine Eintragung im öffentlichen Kundenverzeichnis seine Rufnummer beim Angerufenen angezeigt wird.

Über diese kostenlosen Wahl- und Gestaltungsmöglichkeiten ist der Kunde gemäß § 3 Abs. 5 TDSV bei Vertragsabschluss zu informieren.

Bei der Versendung von SMS wird die Rufnummer als Bestandteil der Absenderadresse immer mit übertragen.

4.5.7.2 Geltung für Corporate Networks

Die Vorschriften zum Datenschutz im TKG richten sich an Personen oder Unternehmen, die geschäftsmäßig Telekommunikationsdienste anbieten (siehe 4.1). Dem entsprechend sind die gesetzlichen Vorschriften unabhängig von der Frage anwendbar, ob eine Gewinnerzielungsabsicht besteht oder nicht. Unerheblich ist es auch, ob Telekommunikationsdienste für die Öffentlichkeit angeboten werden, oder nur für „geschlossene Benutzergruppen“, zu denen die sog. Corporate Networks gehören. Gleichwohl differenziert die neue TDSV in ihren Regelungen dort, wo es sachgerecht und angemessen ist, zwischen geschlossenen Benutzergruppen und den Telekommunikationsunternehmen, die ihre Leistungen gegenüber jedermann anbieten. So brauchen die Vorschriften über die Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung gemäß § 11 Abs. 1 Satz 4 TDSV von den Betreibern geschlossener Benutzergruppen nicht beachtet zu werden.

4.5.7.3 Rufnummernanzeige bei Notrufeinrichtungen

Für Anrufe zu Einrichtungen, die Notrufe unter den Nummern 110, 112, 124 beantworten oder bearbeiten, müssen die Diensteanbieter sicherstellen, dass eine Anzeige der Rufnummer in jedem Fall erfolgt (§ 11 Abs. 6 TDSV).

4.5.8 Anrufweiterschaltung

In § 12 TDSV ist geregelt, dass der Inhaber eines Anschlusses, der Adressat einer automatischen Anrufweiterschaltung ist, die Möglichkeit haben muss, diese Weiterschaltung auf sein Endgerät auf einfache Weise abzustellen, soweit dies technisch möglich ist. Die Diensteanbieter sind verpflichtet, ihren Kunden diese Möglichkeit kostenlos einzuräumen.

4.6 Auskünfte an die Strafverfolgungsbehörden und andere

Für die Arbeit der Strafverfolgungsbehörden, der Polizei und der Sicherheitsdienste ist es oftmals wichtig zu wissen, wer der Anschlussinhaber einer bestimmten Telefonnummer ist oder welche Telefonnummer eine bestimmte Person hat - auch wenn der Anschluss nicht im Telefonbuch eingetragen ist. Nach § 89 Abs. 6 und § 90 TKG haben die Anbieter von Telekommunikationsdiensten derartigen Auskunftsersuchen zu entsprechen.

4.6.1 Auskunftsersuchen im Einzelfall

§ 89 Abs. 6 TKG regelt die Auskunftspflicht für Einzelfallanfragen an Telekommunikations-Diensteanbieter; Auskunft ist zu erteilen über alle personenbezogenen Daten, die von dem Diensteanbieter für die Begründung, inhaltliche Ausgestaltung oder die Änderung des Vertragsverhältnisses erhoben worden sind. Ein für den Telekommunikationsbereich spezialgesetzlich geregeltes „vereinfachtes Auskunftsverfahren“, wie es § 89 Abs. 6 TKG darstellt, erlaubt den Strafverfolgungs- und Sicherheitsbehörden aber keineswegs, alle Vertragsdaten von Telekommunikationskunden, die bei dem Diensteanbieter vorhanden sind, abzufordern. Daten, die keinen spezifischen Telekommunikationsbezug haben, dürfen nach Auffassung des Bundesbeauftragten für den Datenschutz nicht

abgefragt werden, u.a. Angaben über Bankverbindungen oder die Zugehörigkeit zu bestimmten gesellschaftlichen Gruppen, denen z.B. Sondertarife eingeräumt werden.

Die Abrufe sind für die nachfragenden Stellen nach § 17 des Gesetzes über die Entschädigung von Zeugen und Sachverständigen kostenpflichtig.

4.6.2 Automatisiertes Auskunftsverfahren

§ 90 TKG regelt ein Verfahren, mit dem die berechtigten Stellen einen eng begrenzten Teil der Bestandsdaten, die Gegenstand eines Auskunftsersuchens nach § 89 Abs. 6 TKG sein können, über die Regulierungsbehörde für Telekommunikation und Post im Wege eines automatisierten Abrufs erlangen können:

Wer geschäftsmäßig Telekommunikationsdienste anbietet (siehe 4.1 und 4.5.1.2), ist nach § 90 TKG verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere - z.B. sog. Serviceprovider - vergeben werden, sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingenten aufzunehmen sind. Hierbei werden auch die Daten von Kunden erfasst, die nicht in öffentlichen Verzeichnissen eingetragen sind. Die aktuellen Kundendateien sind so verfügbar zu halten, dass die Regulierungsbehörde einzelne Daten oder Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann. Der verpflichtete Kommunikations-Diensteanbieter hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können.

Bedarfsträger, die Auskünfte aus den Kundendateien erhalten können, sind die

- Gerichte, Staatsanwaltschaften und andere Justizbehörden sowie sonstige Strafverfolgungsbehörden,
- Polizeien von Bund und Ländern für Zwecke der Gefahrenabwehr,
- Zollfahndungsämter für Zwecke eines Strafverfahrens sowie das Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes und
- Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst.

Die Auskünfte sind den Bedarfsträgern jederzeit unentgeltlich zu erteilen, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Die Regulierungsbehörde hat die Daten, die in Kundendateien gespeichert sind, auf Ersuchen der

vorgenannten Stellen automatisiert abzurufen und an die ersuchende Stelle zu übermitteln.

Mit dieser Vorschrift wollte der Gesetzgeber dem Umstand Rechnung tragen, dass aufgrund der Liberalisierung des Telekommunikationsmarktes für Auskunftsersuchen über die genannten Daten inzwischen eine Vielzahl von Adressaten in Frage kommt. Um zeitraubende Recherchen darüber zu vermeiden, bei welchem Telekommunikations-Diensteanbieter die gesuchten Daten gespeichert sind, wurde die Rechtsgrundlage für ein automatisiertes Abrufverfahren geschaffen.

Ferner hat der Telekommunikations-Diensteanbieter durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können. Mit der Regelung soll verhindert werden, dass bei den verpflichteten Telekommunikations-Diensteanbietern Spekulationen etwa über die Zuverlässigkeit des betroffenen Kunden angestellt werden und man ihm vorsichtshalber den Vertrag kündigt nach dem Motto: "Wenn sich die Regulierungsbehörde für XY interessiert, bedeutet das nichts Gutes".

Die Regulierungsbehörde gibt aber nicht nur die abgerufenen Daten an die ersuchende Stelle weiter, sondern protokolliert auch bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, die die Daten abrufende Person sowie die ersuchende Stelle und deren Aktenzeichen. Hiermit soll nicht nur bei ihr selbst, sondern auch bei der ersuchenden Behörde eine genaue Datenschutzkontrolle ermöglicht werden. Ruft die Regulierungsbehörde Daten für die Polizei eines bestimmten Bundeslandes ab, kann dessen Landesdatenschutzbeauftragter bei der Polizei kontrollieren, ob das zulässig war. Die Regulierungsbehörde wiederum wird vom Bundesbeauftragten für den Datenschutz hinsichtlich der datenschutzrechtlichen Verpflichtungen beraten und kontrolliert.

Neben dem automatisierten Abrufverfahren können über Name, Anschrift und Rufnummer hinausgehende weitere Bestandsdaten von den Bedarfsträgern weiterhin durch Auskunftsersuchen gemäß § 89 Abs. 6 TKG bei den verpflichteten Telekommunikations-Diensteanbietern erfragt werden.

Im Gegensatz zu dem Verfahren nach § 89 Abs. 6 TKG werden die Abfragen nach § 90 TKG kostenfrei erteilt (siehe 4.6.1).

4.7 Technische Umsetzung von Überwachungsmaßnahmen

Die rechtlichen Grundlagen für die Ermächtigung zur inhaltliche Überwachung der Telekommunikation finden sich nicht im Telekommunikationsgesetz, sondern

- im Gesetz zu Art. 10 Grundgesetz,
- in der Strafprozessordnung und
- im Aussenwirtschaftsgesetz.

§ 88 TKG regelt demgegenüber die technische Umsetzung der Überwachungsmaßnahmen. Gleichzeitig ermächtigt § 88 Abs. 2 Satz 2 TKG die Bundesregierung, eine Rechtsverordnung zu erlassen, die folgende Sachverhalte zum Inhalt hat:

- Die Anforderungen an die Gestaltung der technischen Einrichtungen sowie an die organisatorische Umsetzung von Überwachungsmaßnahmen mittels dieser Einrichtungen,
- das Genehmigungsverfahren und das Verfahren der Abnahme sowie
- die Bestimmungen, bei welchen Telekommunikationsanlagen aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit technische Einrichtungen nicht zu gestalten oder vorzuhalten sind.

Die Telekommunikations-Überwachungsverordnung (TKÜV) verpflichtet die Betreiber von Telekommunikationsanlagen, die ihre Dienste gegenüber jedermann anbieten, technische Einrichtungen zur Umsetzung der gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und vorbereitende organisatorische Vorkehrungen für die Umsetzung dieser Maßnahmen zu treffen. Diese Pflicht richtet sich aber nicht an die Betreiber von Telekommunikationsanlagen, die ihre Dienste nicht für die Öffentlichkeit, sondern nur für bestimmte Dritte anbieten. Hierzu zählen etwa die Nebenstellenanlagen in Hotels, Betrieben oder Krankenhäusern (siehe Anhang 1 II.2).

Bis zum Inkrafttreten der TKÜV galt die Fernmeldeverkehr-Überwachungs-Verordnung (FÜV) von 1995, welche ausschließlich die Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, verpflichtet.

4.8 Kontrolle des Datenschutzes in der Telekommunikation

4.8.1 Überblick über die Kontrollzuständigkeiten

Im Telekommunikationsbereich hat die Regulierungsbehörde für Telekommunikation und Post die Aufgabe, die Einhaltung des TKG und der danach erlassenen Rechtsverordnungen zu kontrollieren und für ihre Durchsetzung zu sorgen (§ 91 Abs. 1 TKG). Hierzu kann sie Anordnungen und Maßnahmen treffen, um die Einhaltung der Vorschriften des Elften Teils des TKG sicherzustellen; dazu gehören auch solche über das Fernmeldegeheimnis (§ 85 TKG) und den Datenschutz (§ 89 TKG).

Die Zuständigkeit für Kontrollen im Bereich des Datenschutzes bei Telekommunikationsunternehmen ist gemäß § 91 Abs. 4 TKG - abweichend von § 38 BDSG - nicht den Datenschutzaufsichtsbehörden der Länder für den nicht-öffentlichen Bereich, sondern dem Bundesbeauftragten für den Datenschutz zugewiesen. Nach dem Willen des Gesetzgebers soll dieser als zentrale Instanz nach bundesweit einheitlichen Maßstäben die Einhaltung von Datenschutzvorschriften durch diejenigen Stellen, die Telekommunikationsdienste erbringen oder daran mitwirken, sicherstellen. Dabei sind auch anlassunabhängige Präventivkontrollen möglich. Durch diese Regelung kommt es zu einer gewissen „Doppelzuständigkeit“ für die Regulierungsbehörde für Telekommunikation und Post und den Bundesbeauftragten für den Datenschutz in diesem Bereich.

Die Kontrollzuständigkeit des Bundesbeauftragten für den Datenschutz beschränkt sich bei den Telekommunikationsdiensteanbietern auf diejenigen personenbezogenen Daten, die im Zusammenhang mit der Erbringung von Telekommunikationsdiensten erhoben, verarbeitet und genutzt werden. Für die darüber hinausgehende Datenverarbeitung dieser Unternehmen (z.B. die Verarbeitung personenbezogener Daten ihrer Mitarbeiter) verbleibt es gemäß § 38 BDSG bei der Zuständigkeit der Aufsichtsbehörden der Länder.

Soweit öffentliche Stellen der Länder Telekommunikationsdienste erbringen, liegt die Kontrollzuständigkeit bei den jeweiligen Landesbeauftragten für den Datenschutz. Wenn also beispielsweise datenschutzrechtliche Probleme im Zusammenhang mit der Nutzung der Telefon-Nebenstellenanlage einer landeseigenen Universität aufträten, wäre hierfür der Landesdatenschutzbeauftragte zuständig.

Die Anschriften der Datenschutzbeauftragten des Bundes und der Länder finden Sie in den Anhängen 10 und 11.

4.8.2 Die datenschutzrechtlichen Kontrollzuständigkeiten im einzelnen

Bei welcher Stelle die datenschutzrechtliche Kontrollkompetenz im Einzelfall liegt, ist aufgrund des jeweils zu beurteilenden Sachverhaltes zu entscheiden. Grundsätzlich muss dabei zunächst zwischen Netzbetreibern und Telekommunikationsdiensteanbietern unterschieden werden. Innerhalb dieser beiden Gruppen ist dann weiterhin wie folgt zu differenzieren:

Netzbetreiber:

- Behördennetze

In Bezug auf die von Behörden betriebenen Telekommunikationsnetze ist bei der datenschutzrechtlichen Kontrollkompetenz danach zu unterscheiden, ob es sich um eine öffentliche Stellen des Bundes oder eines Landes bzw. einer Gemeinde handelt. Für öffentliche Stelle des Bundes ist der Bundesbeauftragte für den Datenschutz zuständig.

Handelt es sich um das Netz einer Landesbehörde bzw. einer Gemeinde, liegt die datenschutzrechtliche Kontrollzuständigkeit entsprechend den einschlägigen Landesdatenschutzgesetzen bei dem jeweils zuständigen Landesbeauftragten für den Datenschutz.

- Privatrechtlich organisierte Netzbetreiber

Gemäß § 91 Abs. 4 TKG obliegt die Kontrolle hier dem Bundesbeauftragten für den Datenschutz, soweit dabei Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden. Dabei ist es unerheblich, ob das Netz mit der Absicht der Gewinnerzielung betrieben wird. § 91 Abs. 4 TKG stellt insoweit lediglich auf einen geschäftsmäßigen Betrieb (siehe 4.5.1.2) im Sinne von § 3 Nr. 5 TKG ab.

Telekommunikationsdiensteanbieter:

- Gewerbsmäßige Telekommunikationsdiensteanbieter

Diejenigen Telekommunikationsdiensteanbieter, die ihre Leistungen für die Öffentlichkeit mit der Absicht der Gewinnerzielung erbringen, unterliegen der datenschutzrechtlichen Kontrolle des Bundesbeauftragten für den Datenschutz. Nach § 91 Abs. 4 TKG tritt bei diesen Anbietern "an die Stelle der Kontrolle nach § 38 des Bundesdatenschutzgesetzes eine Kontrolle durch den Bundesbeauftragten für den Datenschutz entsprechend §§ 21 und 24 bis 26 Abs. 1 bis 4 des Bundesdatenschutzgesetzes".

- Telekommunikationsdiensteanbieter für geschlossene Benutzergruppen

  - Telekommunikationsanlagen von Behörden und anderen öffentlichen Stellen:

    Die datenschutzrechtliche Kontrollkompetenz in bezug auf die von Behörden an ihre Mitarbeiter für die private Nutzung erbrachten Telekommunikationsdienstleistungen beurteilt sich entsprechend den obigen Ausführungen zu den von Behörden betriebenen Telekommunikationsnetzen.

    Demgemäss kontrolliert der Bundesbeauftragte für den Datenschutz die von Bundesbehörden erbrachten Telekommunikationsdienstleistungen, während die Landesbeauftragten für den Datenschutz die Beachtung der einschlägigen datenschutzrechtlichen Vorschriften bei der Leistung von Telekommunikationsdiensten durch landeseigene Behörden kontrollieren.

  - Telekommunikationsanlagen von Firmen, Hotels, Krankenhäusern usw.

    Auch in diesem Bereich erfolgt die Kontrolle durch den Bundesbeauftragten für den Datenschutz.

4.8.3 Maßnahmen bei Verstößen gegen datenschutzrechtliche Bestimmungen

Stellt der Bundesbeauftragte für den Datenschutz bei Telekommunikationsdiensteanbietern Verstöße gegen Datenschutzvorschriften oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies nach § 91 Abs. 4 Satz 2 TKG i.V.m. § 25 BDSG gegenüber dem Bundesministerium für Wirtschaft und Technologie. Er kann darauf verzichten, wenn die Verstöße oder Mängel unerheblich sind oder datenschutzrechtliches Fehlverhalten sofort geändert bzw. die Mängel inzwischen beseitigt wurden.

Die Reaktion auf festgestellte Rechtsverstöße in Form hoheitlicher Maßnahmen obliegt der Regulierungsbehörde für Telekommunikation und Post, die zugleich Verantwortung für die Einhaltung des Fernmeldegeheimnisses sowie für die technische Sicherheit der Telekommunikationsanlagen trägt. Die Regulierungsbehörde kann nach § 91 Abs. 1 TKG Anordnungen und andere Maßnahmen treffen, um die Einhaltung des Elften Teils des TKG und der hierzu ergangenen Rechtsverordnungen (z.B. TDSV) sicherzustellen. Sie ist auch zur Verhängung von Geldbußen nach §§ 96 TKG, 17 TDSV (siehe 3.4.6) befugt. Wenn mildere Maßnahmen nicht ausreichen, kann nach § 91 Abs. 3 TKG sogar der Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagt werden.

4.8.4 Gegenstand, Umfang und Anlass der Kontrollen

Gegenstand und Umfang der beschriebenen Kontrollkompetenz des Bundesbeauftragten für den Datenschutz bei den betroffenen Netzbetreibern bzw. Telekommunikationsdiensteanbietern richten sich nach den einschlägigen Rechtsvorschriften des TKG bzw. der TDSV. Danach bezieht sich die Datenschutzkontrolle ausschließlich auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Zusammenhang mit telekommunikationsrelevanten Vorgängen. Hierzu zählen:

- Akquisition von Telekommunikationsdiensten, soweit diese kundenbezogen erfolgt und dabei personenbezogene Daten erhoben, verarbeitet oder genutzt werden;

- Begründung von Vertragsverhältnissen über Telekommunikationsdienste. Hierzu gehören auch die Feststellung der Identität des Kunden sowie die Prüfung seiner Bonität und sonstige Vorbereitungsmaßnahmen;

- Durchführung von Vertragsverhältnissen, einschließlich der Nutzung personenbezogener Daten für das bedarfsgerechte Gestalten von Telekommunikationsdiensten;

- Verarbeitung und Nutzung von Vertragsdaten für andere als Telekommunikationszwecke, etwa für Zwecke der Eigen- oder Fremdwerbung; Verarbeitung von Verbindungsdaten, z. B. für den Betrieb von Missbrauchserkennungssystemen;

- Verarbeitung von Entgeltdaten zur Rechnungserstellung oder für das Inkasso;

- Veröffentlichung von Kundendaten in öffentlichen Kundenverzeichnissen oder im Rahmen von Auskunftsdiensten;

- Verarbeitung von Bestands-, Verbindungs- und Entgeltdaten im Zusammenhang mit dem Vorhalten von Telekommunikationsverbindungen, z.B. Öffnung eines Internetzuganges zur Nutzung von Telediensten (nicht hingegen Daten im Zusammenhang mit der eigentlichen Teledienstnutzung).

Kontrollanlass können Beschwerden der Kunden von Telekommunikationsdiensteanbietern sein oder sonstige tatsächlichen Anhaltspunkte für die Verletzung datenschutzrechtlicher Vorschriften. Sie sind jedoch keine notwendige Voraussetzung für Kontrollen durch den Bundesbeauftragten für den Datenschutz. Nach § 91 Abs. 4 TKG in Verbindung mit § 24 Abs. 1 BDSG können Telekommunikationsdiensteanbieter auch präventiv kontrolliert werden; der BfD entscheidet hierüber nach eigenem pflichtgemäßen Ermessen. Möglich sind daher z.B. auch Kontrollen aufgrund von Presseveröffentlichungen über neue technische Entwicklungen oder aufgrund von Werbeschriften der Telekommunikationsunternehmen zu neuen Leistungsmerkmalen, die datenschutzrechtliche Fragestellungen aufwerfen; Hinweise auf Rechtsverletzungen müssen also nicht vorliegen.

Die Telekommunikationsdiensteanbieter sind verpflichtet, den Bundesbeauftragten für den Datenschutz bei seiner Kontrolltätigkeit zu unterstützen, ihm die erforderlichen Auskünfte zu erteilen, Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme, zu ermöglichen und ihm jederzeit Zutritt in alle Geschäfts- und Betriebsräume zu gewähren (§ 91 Abs. 4 TKG i.V.m. § 24 Abs. 4 BDSG).

5 Einzelne Datenschutzprobleme in der Telekommunikation

5.1 Telekommunikationsanlagen

Der Einzug der Digitaltechnik im Bereich Telekommunikationsanlagen brachte nicht nur eine Fülle an nützlichen Funktionen, sondern auch fast unbemerkt eine veränderte Gefährdungslage für das Fernmeldegeheimnis. Während bei der alten Analogtechnik die Hardware des Systems, z.B. das Endgerät (Telefon) oder auch das Leitungsnetz, als der Angriffspunkt gesehen werden konnte, rückt bei der digitalen Technik die Software in den Vordergrund. Die Angriffe konzentrieren sich nicht mehr auf die Manipulation der Hardware, z.B. das Anzapfen einer Leitung, sondern bestehen in der missbräuchlichen Nutzung vorhandener Funktionalitäten. Hierzu gehört z.B. das Aufschalten auf bestehende Verbindungen (siehe 4.5.5.3), der unbemerkte Aufbau einer Dreierkonferenz, die Rufumleitung auf einen Fremdapparat oder das direkte Ansprechen (siehe 5.1.4) eines Teilnehmers (Wechselsprechanlage). Diese oder ähnliche Leistungsmerkmale können - vorausgesetzt, entsprechendes Fachwissen ist vorhanden - zum Gebührenbetrug oder Abhören missbraucht werden.

Die Verhinderung des Missbrauchs dieser durchaus gewünschten und 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 die Sicherstellung, dass nur befugtes Personal Veränderungen vornehmen kann. Insbesondere ist die Fernwartung (siehe 7.1.9) in solche Überlegungen mit einzubeziehen. In diesem Zusammenhang ist auf den Katalog von Sicherheitsanforderungen (siehe 4.4) sowie die vom Bundesamt für Sicherheit in der Informationstechnik herausgegebene Publikation „Sicherer Einsatz von digitalen Telekommunikationsanlagen“ zu verweisen, die eine Reihe von nützlichen und hilfreichen Hinweisen zum sicheren Betrieb und (insbesondere für Behörden) zur Beschaffung von Telekommunikationsanlagen enthält. Diese Publikation können Sie in der PDF-Version aus dem Internetangebot des Bundesamtes für Sicherheit in der Informationstechnik herunterladen (http://www.bsi.de/literat/) oder beim Bundesanzeiger-Verlag (Postfach 1320, 53003 Bonn) beziehen.

Nicht benötigte Leistungsmerkmale sollten grundsätzlich deaktiviert werden. Manche TK-Anlagen verfügen über Ländereinstellungen, bei denen auch rechtliche Vorgaben

für die verschiedenen Länder berücksichtigt sind. Es sollte darauf geachtet werden, dass dann auch „Deutschland“ aktiviert ist.

5.1.1 Anrufliste

Neuere Telekommunikationsanlagen besitzen - zum Teil nur für bestimmte Endgeräte - das Leistungsmerkmal "Anrufliste": Von bei einem bestimmten Teilnehmer angekommenen, nicht entgegengenommen Anrufen werden Datum, Uhrzeit und Rufnummer des Anrufers zur Nutzung durch den Angerufenen automatisch in einer "Anrufliste" gespeichert. Die "Anrufliste" wird von vielen gern genutzt, denn nach ihrem Aufruf ist der Rückruf zu einem der Anrufer mit lediglich einem Knopfdruck möglich. Anrufer, die dies alles nicht wissen, sind allerdings häufig über einen solchen Rückruf ("Sie stehen in meiner Anrufliste!") sehr verwundert oder auch verärgert. Dies vor allem dann, wenn sie dem Angerufenen die eigene Rufnummer gerade nicht mitteilen wollten.

Der Eintrag eines Anrufes in die Anrufliste erfolgt nur, wenn der Anrufer das Leistungsmerkmal "Rufnummernübermittlung" besitzt. Dieses kann für eine Telekommunikationsanlage an dieser selbst unterdrückt werden, für Einzelanschlüsse durch den Diensteanbieter bzw. das Telekommunikationsunternehmen. Meist ist es auch am Endgerät möglich die Rufnummernübermittlung generell oder für den nächsten Anruf zu unterdrücken (siehe 4.5.7.1). Soll bei geschlossenen Benutzergruppen die Rufnummer immer übertragen werden, ist den Betreibern von Telekommunikationsanlagen dringend zu empfehlen, alle Nutzer der Anlage sowohl über die Rufnummernübermittlung als auch über die Anrufliste zu informieren (siehe 4.5.7.2) und diese Information in angemessenen Zeitabständen zu wiederholen.

5.1.2 Anzeige der zuletzt gewählten Rufnummer

Sowohl für Endgeräte von Telekommunikationsanlagen als auch bei modernen Telefonen an Einzelanschlüssen wird die zuletzt gewählte Rufnummer zumeist gespeichert, damit sie - z.B. weil der Anrufer nicht erreicht werden konnte - für die Funktion "Wahlwiederholung" genutzt werden kann. Bei manchen Telekommunikationsanlagen wird durch die Vorwahl einer sogenannte PIN (Personal

Identification Number) ein danach gewähltes Gespräch als Privatgespräch gekennzeichnet.

Einige Endgeräte, aber auch manche Telekommunikationsanlagen, speichern jedoch nicht nur die zuletzt eingegebene Telefonnummer einer gewünschten Verbindung, sondern alle eingegebenen Ziffern - auch die PIN zum Aufschließen des "elektronischen Telefonschlosses" oder die PIN eines externen Anrufbeantworters. Dadurch kann eine PIN durch Betätigung der Wahlwiederholungstaste abgerufen und - sofern sich ein Display am Telefonapparat befindet - auch ausgespäht und unbefugt genutzt werden.

5.1.3 Lauthören

Nicht unproblematisch ist die Nutzung des heute bei vielen Telefonen vorhandenen Lautsprechers, wenn er ohne Wissen des anderen Gesprächsteilnehmers heimlich eingeschaltet wird und weitere im Raum anwesende Personen mithören können. Häufig ist daher gefordert worden, dass dies dem Kommunikationspartner zumindest - z.B. durch einen Hinweiston - signalisiert werden müsste; leider hat bisher weder der zuständige Verordnungsgeber dem Rechnung getragen noch ist dies von der Industrie realisiert worden.

Die Mitarbeiter in den Behörden und Betrieben sollten angewiesen werden, eine Lautsprecherzuschaltung stets von der Einwilligung des Telefonpartners abhängig zu machen.

5.1.4 Direktansprechen / Direktantworten

Viele Endgeräte sind mit der Möglichkeit des Freisprechens ausgerüstet, d.h., zum Führen eines Telefonates braucht der Hörer nicht abgenommen zu werden; es braucht lediglich ein Knopf („Leitungstaste“) 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 und Sekretärin eingerichtet, häufig wird es aber auch in Teamfunktion gewünscht: Der Chef kann damit kurze Rückfragen an seine 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, empfiehlt der Bundesbeauftragte für den Datenschutz dringend, bei Nebenstellenanlagen dieses Leistungsmerkmal nur dort freizuschalten, wo es dringend benötigt wird und die Betroffenen informiert sind. Beim Direktansprechen muss ein optisches und akustisches Signal erzeugt werden und wenn möglich das Leistungsmerkmal „Ansprechschutz“ zur Verfügung stehen. Wird letzteres aktiviert, ist ein Direktansprechen dieses Anschlusses nicht möglich.

5.1.5 Konferenzschaltung

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

5.1.6 Zeugenzuschaltung

Manche Telekommunikationsanlagen verfügen auch über das Leistungsmerkmal „Zeugen zuschalten“. Dabei wird ein anderer Teilnehmer oder ein Tonbandgerät unbemerkt in eine bestehende Verbindung eingeschaltet. Der Einsatz dieses Leistungsmerkmals ist in der Bundesrepublik nicht zulässig, da eine Tonbandaufnahme nach § 201 Abs. 1 Nr. 1 StGB strafbar wäre.

Eine Ausnahme für das Mitschneiden von Anrufen kann nur für Drohanrufe gelten. In manchen Behörden und Unternehmen kann bei der Telefonzentrale ein Aufzeichnungsgerät zugeschaltet werden, sobald ein Gespräch als Drohanruf, z. B.

eine Bombendrohung, erkannt wird. Solche Ausnahmen können aber nur für sicherheitskritische Bereiche gelten.

5.1.7 „Mitschneiden“ auf Anrufbeantworter

So genannte Komforttelefone verfügen oftmals über eine Funktion, die es ermöglicht, während eines laufenden Gesprächs den eingebauten Anrufbeantworter zu aktivieren und so das Gespräch aufzuzeichnen (mitzuschneiden). Dies ist nur zulässig, wenn zuvor der Gesprächspartner in die Aufzeichnung eingewilligt hat. Andernfalls würde der Aufzeichnende eine Straftat begehen, die nach § 201 Abs. 1 Nr. 1 StGB mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe geahndet werden kann. Dies ist den meisten Käufern solcher Komforttelefone nicht bewusst, zumal ein entsprechender Hinweis in den Bedienungsanleitungen für diese Geräte meist nicht enthalten ist. Hier gilt jedoch der Grundsatz „Unwissenheit schützt vor Strafe nicht“.

5.1.8 Raumüberwachung

Manche Komforttelefone, Anrufbeantworter oder Telefonanlagen bieten auch die Möglichkeit, durch einen Anruf (von außerhalb nach Eingabe eines persönlichen Identifizierungscodes oder in einer TK-Anlage durch Vorwahl einer Kennzahl) das Mikrofon eines Komforttelefons zu aktivieren. Diese Funktion, auch als Babyphone bezeichnet, soll der Raumüberwachung dienen, z.B. um vom Urlaubsort aus zu prüfen, ob sich jemand unbefugt in der Wohnung aufhält. Wer allerdings diese Raumüberwachungsmöglichkeit - evtl. mit Hilfe einfacher Manipulationen - dazu missbraucht, in seiner Wohnung nicht für seine Ohren bestimmte Gespräche oder die Unterhaltung in einem Büro eines Kollegen heimlich mitzuhören, kann sich ebenfalls nach § 201 Abs. 2 StGB strafbar machen.

5.2 Abhörgefahr bei Funkdiensten

5.2.1 Schnurlose Telefone

Die Zeiten, in denen es nur eines einfachen Scanners, d.h. eines in jedem Fachgeschäft erhältlichen Spezialempfängers bedurfte, um schnurlose Telefone abzuhören, sind mit digitalen DECT-Telefonen weitgehend vorbei. Der technische Aufwand für das Abhören von Gesprächen auf der Luftschnittstelle ist hier enorm. Dies beruht zunächst einmal auf dem Umstand, dass die Nachrichten auf dem Funkweg nicht mehr analog, sondern digital übertragen werden. Ein einfaches Abhören mit preiswerten Geräten ist also nicht mehr möglich. Wer ein besonders hohes Sicherheitsbedürfnis hat, sollte sich ggf. beim Hersteller über die Verschlüsselungsverfahren informieren, die er für seine Telefonate nutzen kann.

Dies gilt jedoch nicht für (meist ältere) schnurlose Telefone nach dem CT1+ Standard oder für andere (nicht zugelassene) analoge schnurlose Telefone. Diese sind mit einfachen Mitteln abhörbar.

5.2.2 Handys

In den Mobilfunknetzen nach dem GSM-Standard (D1-, D2-, ePlus- und Viag-Interkom-Netz) werden Sprache und Daten digital übertragen. Zusätzlich wird mit einem kryptographischen Algorithmus verschlüsselt, wobei der Schlüssel häufig gewechselt wird. Dies gilt nicht nur für die Gesprächsinhalte, auch die Teilnehmerkennung wird in der Regel nicht im Klartext übertragen. Das heißt, wer Datenpakete eines Gesprächs auf der Luftschnittstelle abfängt, kann nicht ermitteln, wer der Urheber der Daten ist. Alle diese Mechanismen führten dazu, dass das Handy, zumindest was das Mithören der Telefongespräche betrifft, als sehr sicher gilt.

In besonderen Fällen, z. B. in manchen ausländischen Netzen, ist die Verschlüsselung nicht aktiv. Dann ist ein Mithören - aber immer noch mit einem sehr hohen Aufwand - möglich.

5.2.2.1 Handy als Wanze

Wenn der Besitzer bei seinem Handy zwei Leistungsmerkmale gleichzeitig aktiviert - dies ist bei vielen Handymodellen möglich - und eine transportable Freisprecheinrichtung – im Laden für ein paar Mark zu kaufen – anschließt, kann er dieses als unauffällige Abhöreinrichtung einsetzen. Wenn das so vorbereitete Handy von einem anderen Telefon aus angerufen wird, schaltet es ohne zu klingeln das Mikrofon ein. Gespräche in dem Raum, in dem sich das Handy befindet, können dann von außen mitgehört werden. Dabei ist die Übertragungsqualität überraschend gut.

Bei einem normalen Handy kann man dabei am Display eine bestehende Verbindung erkennen. Es besteht jedoch auch die Möglichkeit, dass einem Abhöropfer ein umgebautes Gerät untergeschoben wird, bei dem das Display keine Aktivität anzeigt, während die Raumgespräche abgehört werden. Es kann daher ratsam sein, bei wichtigen persönlichen Gesprächen das Handy auszuschalten.

5.2.2.2 Ortung

Seit einiger Zeit gibt es auch Ortsbezogene Dienste, sogenannte Location Based Services. Hier kann man sich über WAP (Wireless Access Protocol) beispielsweise die Hotels in der näheren Umgebung auflisten lassen. Dazu muss der Netzbetreiber den Standort bestimmen und die gewünschten Informationen bei einer - evtl. externen - Datenbank abfragen. Hier kann es empfehlenswert sein, sich bei seinem Netzbetreiber über die Verarbeitung der Ortsinformationen zu informieren.

Bei normalen Handygesprächen kann, wenn ein günstiger „Ortstarif“ angeboten wird, der Standort einen deutlichen Preisunterschied bedeuten. Hierfür muss der Netzbetreiber zunächst den Ort bestimmen und diese Information speichern, um dann den richtigen Tarif zu berechnen. Anhand eines Einzelverbindungsnachweises ist dann auch feststellbar, dass sich der Anrufer in dieser Stadt befunden hat.

5.2.2.3 SMS

Bei einem Telefonat kann der Anrufer bestimmen, ob seine Rufnummer übertragen wird oder nicht (siehe 4.5.7). Bei Kurzmitteilungen (SMS) wird die Rufnummer immer

übertragen. Dies mag Handybesitzern, die diesen Dienst nur gelegentlich nutzen, nicht bewusst sein und kann somit zu einer ungewollten Weitergabe der Handynummer führen.

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

5.2.2.4 Handyreparatur

Bei einem Handy mit zusätzlichen Komfortmerkmalen, wie z. B. einem Adressbuch oder Terminkalender, werden viele persönliche Daten im Gerät gespeichert. Bei einer eventuell notwendigen Reparatur sollten sensible Daten gelöscht werden oder mit dem Händler geklärt werden, was zu tun ist. Oft erhält man ein Austauschgerät, während das eigene Handy später nach einer Reparatur an einen anderen Kunden weitergegeben wird.

5.2.2.5 Neue Dienste

Ein Handy, das bisher nur zum Telefonieren diente, kann dank neuer Fähigkeiten zur Kommunikationszentrale werden. Dabei speichert es Adressen, Termine, nimmt über die Infrarotschnittstelle oder Bluetooth Kontakt zu anderen Geräten auf und ermöglicht, dank WAP, auch unterwegs den Kontakt zum Internet. Gefahren wie Viren oder Trojaner, die bisher nur bei PCs zu beachten waren, werden auch bei Handys zu berücksichtigen sein, wenn aktive Inhalte ausgeführt werden können. Es ist auch denkbar, dass eine falsch konfigurierte Bluetooth-Schnittstelle Möglichkeiten für Angriffe bietet. Der Anwender sollte sich also mit den neuen Diensten vertraut machen.

5.2.3 Funkrufdienste

Über sogenannte Funkrufdienste (z.B. Cityruf, Scall, Skyper, Telmi) ist es möglich, den Besitzern eines Funkrufempfängers, auch Pager genannt, eine Zahlen- oder Textnachricht zukommen zu lassen. Diese Nachrichten werden in der Regel nach allgemein bekannten Telekommunikationsnormen unverschlüsselt übermittelt und können mit Hilfe üblicher Empfänger von technisch Interessierten, die sich über das Abhörverbot § 86 TKG hinwegsetzen und damit strafbar machen (siehe 4.3), abgehört werden. Auf diese besondere Abhörgefahr sollten die Nutzer von Funkrufdiensten bei Vertragsabschluss deutlich hingewiesen werden.

5.3 Mehrwertdienste

Es gibt verschiedene Mehrwertdienste. Die bekanntesten sind kostenlose 0800er Dienste („Free-Phone“), „Shared-Cost“-Dienste, die mit 0180 beginnen und die teureren 0190er- bzw. 0900er- „Premium-Rate“-Dienste.

Die kostenlosen Gespräche über eine 0800er-Rufnummer dürfen nicht auf dem Einzelverbindungsnachweis des anrufenden Anschlussinhabers aufgeführt werden, da diese nicht gebührenrelevant sind (siehe 4.5.4.1). In Einzelfällen wurden diese dennoch aufgeführt wurden, was beispielsweise bei der Telefonseelsorge, die z. T. über kostenfreie 0800er-Nummern erreichbar ist, sehr bedenklich sein kann.

Bei den Premium-Rate-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 0190er- und 0900er-Rufnummern kann es zu sehr hohen Telefonrechnungen kommen. Bei der Feststellung, welche Rufnummer die Kosten verursacht hat, hilft die Bestimmung des § 7 Abs. 3 Satz 4 TDSV, wonach diese Mehrwertdiensterufnummer grundsätzlich ungekürzt gespeichert werden dürfen (siehe 4.5.3.1). Nach § 43a TKG hat Jedermann gegenüber der Regulierungsbehörde für Telekommunikation und Post (Anschrift und Rufnummer siehe 2.4) einen Anspruch auf Auskunft über Namen und Anschrift eines Anbieters, der Dienstleistungen über eine 0190er- oder 0900er-Rufnummer anbietet. Einzelheiten können auf der Internetseite der Regulierungsbehörde unter www.regtp.de nachgelesen werden.

5.4 Rund um das Internet

Das Internet bietet vielfältige Informationsmöglichkeiten aber auch viele Gefahren, wie Computerviren oder Trojaner. Obwohl die datenschutzgerechte Nutzung des Internets nicht Gegenstand dieser Broschüre ist, soll auf die beiden folgenden Punkte besonders hingewiesen werden, da sie einen unmittelbaren Bezug zu den Telekommunikationsdiensten aufweisen:

- Sprache wird heute grundsätzlich digital übertragen - bei einer guten Anbindung geht dies auch über das Internet, wenn auch meist mit schlechterer Qualität (Stichwort: Voice over IP). Hierbei sollte man sich bewusst sein, dass die Vertraulichkeit im Internet nicht im gleichen Maße gewährleistet ist, wie im Telefonnetz und dass im Ausland andere Regelungen für die Verarbeitung von Verbindungsdaten gelten können.

- Bei einer Einwahl in das Internet über ein Modem wird die Nummer des Internetproviders gewählt und die Verbindung hergestellt. Mit kostenpflichtigen Diensten ist es auch möglich, über das Modem eine 0190-er Nummer anzuwählen und damit den Anbieter für besondere Dienste zu bezahlen. Dabei sollte man die Kosten im Auge behalten und prüfen, ob bei einer späteren Anwahl wieder der gewohnte Anbieter angewählt wird - ansonsten kann es zu sehr hohen Telefonrechnungen kommen (siehe Nr. 5.3).

Wenn Sie an weiteren Informationen zu Aspekten des Datenschutzes im Internet interessiert sind, wird empfohlen, die vom Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder herausgegebene Informationsbroschüre zu dem Thema „Datenschutz bei der Nutzung von Internet und Intranet“, welche sie beim Bundesbeauftragten für den Datenschutz unentgeltlich beziehen können.

5.5 Inverssuche (Anschlussermittlung anhand der Telefonnummer) auf CD-ROM

Auf dem deutschen Markt sind in der Vergangenheit unzulässigerweise CD-ROM-Telefonverzeichnisse vertrieben worden, mit denen sich nicht nur anhand des Namens die Telefonnummer eines bestimmten Anschlussinhabers ermitteln ließ. Aufgrund der auf der CD-ROM angebotenen Suchkriterien war es vielmehr auch möglich, **umgekehrt** - nach Eingabe einer Telefonnummer - Auskunft darüber zu erhalten, wer der Inhaber des Anschlusses ist (so genannte **Inverssuche**), ggf. zusätzlich noch, wo dieser wohnt bzw. welchen Beruf er hat. Die Herausgabe einer

solchen CD-ROM ist entsprechend § 14 Abs. 4 TDSV unzulässig. Würde ein Telekommunikationsdiensteanbieter in Deutschland ein derartiges CD-ROM-Telefonverzeichnis anbieten, würde der Bundesbeauftragte für den Datenschutz hiergegen einschreiten.

Würde eine solche CD-ROM dagegen von einem deutschen Unternehmen, das nicht Telekommunikationsdiensteanbieter ist, vertrieben, wäre dafür die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des jeweiligen Bundeslandes zuständig, in dem das Unternehmen seinen Sitz hat (siehe Anhang 11). Die Aufsichtsbehörden vertreten ebenfalls die Auffassung, dass die Herausgabe solcher CD-ROM-Telefonverzeichnisse datenschutzrechtlich unzulässig ist.

5.6 Telefax

Wer einen Brief verschickt, kann in der Regel darauf vertrauen, dass dieser seinen Empfänger erreicht oder zumindest nicht in falsche Hände gerät. Auch wenn der Empfänger verzogen sein sollte, sorgt die Post dafür, dass der Brief entweder nachgesandt oder als unzustellbar an den Absender zurückgegeben wird. Bei einem Telefonat kennen sich die Gesprächspartner oder stellen sich vor. Verwählt sich ein Anrufer, wird das eigentliche Gespräch erst gar nicht begonnen, man gibt also keine Inhalte preis.

Oberflächlich betrachtet geht dies beim Fax-Verkehr nicht viel anders: Das Fax wird an eine bestimmte Adresse gesandt, in dem eine Telefonnummer eingegeben wird, von der ausgegangen wird, dass unter ihr das Faxgerät des Empfängers erreicht werden kann. Bevor die Übertragung der eigentlichen Nachricht beginnt, tauschen die beteiligten Geräte untereinander Informationen zur gegenseitigen Identifizierung aus, anhand derer im Zweifelsfall vom Absender die Übertragung abgebrochen werden kann.

Und doch gibt es wesentliche Unterschiede zwischen Fax-Verkehr und Briefpost bzw. Telefonat: Ein Fax kommt beim Empfänger gewöhnlich offen – also wie eine Postkarte – an und ist damit für jeden lesbar, der sich in der Nähe des empfangenden Faxgerätes befindet. Nicht sicher ist der Identifizierungsvorgang zwischen den auch heute noch vorwiegend eingesetzten Faxgeräten: Sie identifizieren sich mit der Rufnummer, die ihnen von ihrem Besitzer einprogrammiert wurde und die deshalb veraltet oder manipuliert sein kann. Erst ISDN-Faxgeräte übermitteln einander die „echten“ Rufnummern.

Bereits 1991 hat der Bundesbeauftragte für den Datenschutz in einem Rundschreiben an die obersten Bundesbehörden ausführliche Hinweise für die sichere Nutzung von Telefaxgeräten gegeben und das Muster eines entsprechenden Merkblattes versandt, das nach wie vor aktuell ist (siehe 7.2.2). Gleichwohl kommt es im Fax-Verkehr immer wieder zu Problemen.

5.6.1 Rufnummernänderung

Hat ein Kunde eine neue Faxnummer erhalten, wird in aller Regel eine Information wirklich aller Partner über die neue Nummer kaum möglich sein, da die alte Rufnummer vermutlich im Laufe der Zeit „breit“ gestreut wurde. Wird nun die alte Faxnummer zu rasch einem neuen Kunden zugewiesen, erhält der neue Anschlussinhaber vermutlich noch lange Zeit Faxsendungen, die nicht für ihn bestimmt sind. Dies kann insbesondere bei sensiblen Bereichen (z.B. Behörden, Krankenhäuser, Ärzte, Rechtsanwälte, Steuerberater, Politiker) zu gravierenden Datenschutzverletzungen führen. Nach Auffassung des Bundesbeauftragten für den Datenschutz sollte zumindest in diesen Fällen die Rufnummer eines gekündigten Telefonanschlusses – an den eben (auch) Faxgeräte angeschlossen sein können – frühestens nach 12 Monaten neu vergeben werden.

Allerdings bleibt auch bei einem Rufnummernwechsel des Empfängers der Absender dafür verantwortlich, dass seine Faxsendung den richtigen Empfänger erreicht. Deshalb wird in diesem Zusammenhang empfohlen, regelmäßig und in kürzeren Zeitabständen die Rufnummern der Faxpartner auf Richtigkeit zu überprüfen. Dabei ist zu beachten, dass öffentliche Telefaxverzeichnisse allenfalls halbjährlich neu erscheinen und die jährliche Veränderungsquote bei Telefon-/Telefaxanschlüssen hoch ist.

5.6.2 Falschwahl

Will man ein Telefongespräch führen und macht einen Fehler beim Wählen der Telefonnummer, so hat das im Allgemeinen keine weiteren negativen Folgen. Will man hingegen ein Fax absenden und verwählt sich dabei, können weitreichende Folgen eintreten, wenn durch Zufall unter der falsch gewählten Rufnummer – auch – ein Faxgerät erreicht wird. Die Sendung gelangt dann an einen unerwünschten Empfänger, der möglicherweise personenbezogene oder andere besonders schützenswerte Daten zur Kenntnis nehmen kann.

Wie die in den letzten Tätigkeitsberichten des Bundesbeauftragten für den Datenschutz aufgeführten Beispiele zeigen, ist der Betrieb von Faxgeräten an Telekommunikationsanlagen immer dann eine besondere Fehlerquelle, wenn vor der gewünschten Rufnummer die Ziffer „0“ zur Amtsholung gewählt werden muss, um eine Verbindung ins öffentliche Netz herstellen zu können. Wird vergessen, diese „0“ zusätzlich zu wählen, wird die „0“ einer Vorwahl als Amtsholung von der Telekommunikationsanlage gewertet und die anschließende Ziffernfolge als eigentliche Rufnummer gewählt. Eine Reihe von Eingaben an den Bundesbeauftragten für den Datenschutz zeigen, dass solche Fehler durchaus realistisch sind und durch eindeutige interne Arbeitsanweisungen minimiert werden sollten. Auf jeden Fall sollten alle Faxgeräte einer Stelle einheitlich konfiguriert sein, so dass nicht an manchen Geräten zunächst die „0“ eingegeben werden muss, während bei anderen Geräten diese Kennziffer bereits automatisch vorgewählt wird, um in das öffentliche Telefonnetz zu gelangen.

5.6.3 Einsatz von Fax-Servern

Fax-Server als Bestandteil von PC-Netzen ermöglichen es jedem dazu berechtigten Nutzer, vom eigenen Arbeitsplatz aus z. B. Briefe per Fax zu verschicken.

Das Versenden von Faxdokumenten auf diese Art und Weise erspart in jedem Fall eigene Arbeitszeit und oft auch Versandkosten, ist aber auch mit allen Risiken des „konventionellen“ Faxversandes behaftet. So gestattet die Fax-Software üblicherweise das Anlegen sog. Faxbücher, in denen häufig genutzte Faxrufnummern – oft nach Adressengruppen geordnet – verzeichnet sind und per Maus-Klick (als Sendeziel) ausgewählt werden können. Wenn jedoch nicht durch strikte Organisation die Aktualität der Faxbücher gesichert wird, sind Fehlsendungen vorprogrammiert. Faxgeräte haben im Allgemeinen ein Display, auf dem auch die vom angewählten Faxgerät zurückgesendete Anschlusskennung angezeigt wird und überprüft werden kann. Beim Einsatz von Fax-Servern oder PC mit Faxkarte und entsprechender Software ist diese Möglichkeit meist nicht gegeben. Weil dann eine Falschwahl auch nicht mehr anhand der zurückgesandten Anschlusskennung des erreichten Faxpartners erkannt werden kann, ist hier bei der Eingabe der Rufnummern besondere Sorgfalt geboten. Das Protokoll über den Versand sollte sehr genau kontrolliert werden.

Faxgeräte bieten die Möglichkeit, einen bereits begonnenen Sendevorgang – durch Drücken der dafür vorgesehenen Taste – abzubrechen, wenn beispielsweise eine Falschwahl festgestellt wurde. Die auf Fax-Servern oder Fax-PC installierte Software

bietet zwar die Möglichkeit, einen Sendevorgang erst dann zu starten, wenn der Bediener ein letztes „OK“ gegeben hat. Hat er es aber einmal gegeben, ist er - besonders bei Fax-Servern, auf die er im Allgemeinen keinen direkten Zugriff hat – nicht mehr in der Lage, den Sendevorgang noch abzubrechen. Besonders beim Fax-Versand an Adressatengruppen kann das fatale Folgen haben, wenn dem Absender nach Auslösung des Sendevorganges bewusst wird, dass das Fax eigentlich an eine andere als die gewählte Gruppe hätte abgesandt werden sollen.

5.6.4 Übertragung von Programmen

Mit üblichen Faxgeräten können lediglich optisch lesbare Vorlagen übertragen werden. Mittels eines Fax-Servers oder eines PC’s mit geeigneter Fax-Karte und der entsprechenden Software können dem gegenüber alle Arten von Dateien übertragen werden, also auch „ausführbare Dateien“, nämlich Programme. Vorteile für den Absender sind die schnellere Bearbeitung durch die Fax-Software und eine kürzere Sendezeit und damit Kostenersparnis.

Damit wurde auch im Faxbereich eine Gefährdungsmöglichkeit eröffnet, die bislang lediglich bei klassischen Formen der Datenübertragung zwischen Rechnern bestand: Das Eindringen von schädlichen Programmen (Viren, trojanischen Pferden usw.) z.B. in das PC-Netz des Empfängers. Dabei kann beispielsweise ein Virus auch übersandt werden, ohne dass der Absender sich dessen bewusst ist oder es gar will.

Hier sind sorgfältig geplante, wirksame Abwehrmaßnahmen unerlässlich. Das Bundesamt für Sicherheit in der Informationstechnik – BSI – (Postfach 20 03 63, 53133 Bonn, Tel.: 0228/9582-0) verfügt über Fachleute, die Beratungen zum Schutz gegen Viren und andere schädliche Programme durchführen und Hilfe erteilen.

5.6.5 Fortentwicklung des Faxverkehrs

Die technische Entwicklung wird auch den Faxdienst verändern, bis er vermutlich durch E-Mail und andere Nachrichtenübermittlungsstandards verdrängt sein wird. Bis dahin wird aber noch einige Zeit vergehen und man wird mit den damit verbundenen Risiken leben müssen. Deshalb sollten die Hinweise des Bundesbeauftragten für den Datenschutz aus dem Jahre 1991 (siehe 7.2.2) beachtet werden, da sie nach wie vor ihre Gültigkeit haben.

Da der Teufel bekanntlich im Detail steckt, wird empfohlen, den Fax-Verkehr auf jeden Fall in einer entsprechenden Anweisung zu regeln, alle technischen Sicherheitsoptionen von Fax-Geräten und rechner-gestützten Fax-Anwendungen konsequent zu nutzen sowie vor jeder Übermittlung personenbezogener oder anderer besonders schützenswerter Daten per Telefax äußerst kritisch zu prüfen, ob sie auf diesem Wege notwendig und vertretbar ist.

5.6.6 Faxwerbung

Wie aus einer Reihe von Bürgereingaben deutlich wird und auch der Presse zu entnehmen ist, stellt die unerwünschte Übersendung von Faxen ein ernstes Problem dar. Manche Fax-Besitzer werden mit unverlangten Werbeofferten regelrecht „zugemüllt“. Diese verursachen hohe Kosten für Toner und Papier. Wer allerdings auf die Offerten reagiert, muss noch tiefer in die Tasche greifen, da für solche Fax-Abrufe fast 4,00 DM Telefongebühren pro Minute entstehen können und oftmals ewig dauern.

Dabei ist die Rechtslage zum Thema Werbung eindeutig: Unverlangte Reklame per Fax sind unzulässig, wenn zwischen Firma und Werbeempfänger keine geschäftlichen Beziehungen bestehen. Doch leider kümmert dies unseriöse Werber wenig. In vielen Fällen verschweigen solche Anbieter ihre Anschrift oder tarnen ihre Identität durch eine Briefkastenadresse.

Die nachfolgend aufgeführten Ratschläge bieten zwar keinen absoluten Schutz vor unerwünschter Werbung, helfen aber vielleicht doch, um Fax-Papier, Toner und Nerven zu sparen:

- Bei der Bestellung von Waren sollte man der Nutzung seiner personenbezogenen Daten für Zwecke der Werbung oder Marktforschung schriftlich widersprechen.

- Es sollte gut überlegt werden, die Fax-Nummer in Telefonverzeichnissen zu veröffentlichen.

- Bei einer ISDN-Anlage können durch entsprechende Konfiguration Faxe ohne erkennbare Anrufnummer abgewiesen werden.

- Man kann sich gegen die Werbung per Fax in eine so genannte „Robinson-Liste“ eintragen lassen. Der Vollständigkeit halber sei darauf hingewiesen,

dass die Nutzung dieser Listen durch die Werbewirtschaft freiwillig ist. Ein Eintrag dort garantiert nicht, dass man dadurch absolut werbefrei wird.

Eine solche Liste gegen Werbung per Fax wird vom Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V. (BITKOM) durch die Firma Retarus Network Services GmbH geführt. Ein Antragsformular kann unmittelbar per Fax unter der Telefax-Nr.: 01805/00 07 61 abgerufen werden.

- Bei besonders schwerwiegenden Belästigungen kann man bei seinem TK-Unternehmen eine so genannte Fangschaltung beantragen (siehe 4.5.6).

- Wenn nichts mehr hilft, bleibt leider nur noch die Beantragung einer neuen Fax-Nummer, da der Rechtsweg mühsam ist und keine Erfolgsgarantie bietet.

5.7 E-Mail

Elektronische Post, oder auch E-Mail genannt, wird von immer mehr Menschen genutzt. Ob privat oder geschäftlich, E-Mails sind schnell geschrieben, schnell beim Empfänger und sehr kostengünstig. Deshalb werden sie immer beliebter. Allerdings gehören E-Mails zu den unsichersten Formen der elektronischen Kommunikation. Ist man sich bei der Postkarte noch bewusst, dass deren Inhalt für jedermann lesbar ist, sind die Risiken bei E-Mails viel höher. E-Mails werden auf ihrem Weg durch das weltweite Internet auf verschiedenen Servern zwischengespeichert und passieren Stationen, an denen man sie abfangen, mitlesen oder auch verändern kann. Außerdem ist nicht sicher, dass eine E-Mail von demjenigen stammt, dessen Name und Adresse vom Mailprogramm angezeigt werden.

Da es aber Möglichkeiten gibt, sich mit einfachen Mitteln vor solchen Risiken zu schützen, sollte man sich nicht mit Sorglosigkeit oder mit der oft beobachteten „Es-wird-schon-gutgehen“-Einstellung im Internet bewegen. Die Verschlüsselung, die jedermann zur Verfügung steht, ist ein einfacher Weg, um E-Mails vertraulich zu machen. So wie man einen Brief ganz selbstverständlich in einen Briefumschlag steckt und verschließt, ist die Verschlüsselung nichts anderes als ein elektronischer Briefumschlag. Mit einem Unterschied: Öffnen kann ihn nur der Empfänger. Solche Verschlüsselungsprogramme werden für den nicht-kommerziellen Gebrauch kostenlos angeboten, zum Beispiel PGP (Pretty Good Privacy). Ferner kann man E-Mails mit einer digitalen Signatur „elektronisch unterschreiben“, so dass der Empfänger sicher sein kann, dass die E-Mail auch wirklich vom jeweiligen Absender stammt und unverändert bei ihm eingegangen ist. Im 16., 17. und 18.

Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gibt es hierzu ausführliche Erläuterungen (siehe Anhang 8).

Aber unabhängig davon bleibt das oberste Gebot: Der Nutzer sollte sich immer genau überlegen, welche persönliche Daten oder Informationen er im Netz bekannt machen möchte.

6 Datenschutzfreundliche Technologien in der Telekommunikation

Den Erfordernissen des Datenschutzes wäre nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatsphäre des Einzelnen lediglich auf eine Beschränkung des Zugangs zu seinen bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduzieren würde. Daher ist in § 3 Abs. 4 Telekommunikations-Datenschutzverordnung bestimmt, dass die Telekommunikations-Diensteanbieter sich an dem Ziel der Datenvermeidung und Datensparsamkeit auszurichten haben. Dies betrifft sowohl die technischen Anlagen als auch die Datenverarbeitungsprozesse der Telekommunikation. Demnach sind Art und Umfang der Datenerhebung und –speicherung auf das für Telekommunikationszwecke erforderliche Maß zu beschränken.

Der Bundesbeauftragte für den Datenschutz begrüßt daher erste Entwicklungen, die in diese Richtung zielen, so beispielsweise die sog. Prepaid Cards, bei denen ein vorausbezahlter Geldbetrag auf einen internen Chip gespeichert wird und abtelefoniert werden kann, so dass die Speicherung von Verbindungsdaten zu Abrechnungszwecken entfällt. Ein optimierter Datenschutz erfordert ein weiteres, vermehrtes Angebot, Telekommunikationsdienste pseudonym oder anonym nutzen zu können. Hier sind die Telekommunikationsdiensteanbieter gefordert, entsprechende Produkte zu entwickeln und ihren Kunden anzubieten. Vergleiche hierzu auch die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 (siehe Anhang 5).

Konkretere Überlegungen zu datenschutzfreundlichen Technologien in der Telekommunikation hat der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder formuliert. Diese Broschüre kann beim Bundesbeauftragten für den Datenschutz kostenfrei bestellt werden.

6.1 Call-Center

Viele Unternehmen bedienen sich sog. Call-Center zur Beantwortung von Kundenanfragen. Call-Center sind Telefonauskunfts- und -beratungszentralen, die sich hochtechnisierter kommunikationstechnischer Anlagen bedienen.

Von großer datenschutz- und strafrechtlicher Relevanz ist insbesondere die Frage, ob Kundengespräche mit den jeweiligen Beratern des Call-Centers durch z.B. einen Teamleiter **mitgehört** oder **aufgezeichnet** werden dürfen, um die Qualität der Kundenbetreuung durch die Call-Center-Mitarbeiter zu überprüfen.

Die Datenschutz-Aufsichtsbehörden der Länder und der Bundesbeauftragte für den Datenschutz vertreten einvernehmlich die Auffassung, dass eine **Aufzeichnung** von Gesprächen nur nach vorheriger Einwilligung des Kunden und des Mitarbeiters in Betracht kommt. Eine **Aufzeichnung** ohne eine solche Einwilligung ist grundsätzlich nach § 201 Strafgesetzbuch als „Verletzung der Vertraulichkeit des Wortes“ strafbar. Beim reinen **Mithören** eines Kundengespräches zur Qualitätskontrolle oder zu Ausbildungszwecken empfiehlt der Bundesbeauftragte für den Datenschutz, den Anrufer und den Mitarbeiter des Call-Centers vorher darüber zu informieren. Der Anrufer kann dann selbst entscheiden, ob er das Telefonat fortsetzt oder beendet.

7 Hinweise für die öffentlichen Stellen des Bundes zur Beschaffung und zum Betrieb von Telekommunikationsanlagen

Die nachfolgenden Empfehlungen sind an öffentliche Stellen des Bundes gerichtet. Aus ihnen lassen sich aber auch Anregungen für die Gestaltung und den Betrieb privater Telekommunikationsanlagen entnehmen. Die Hinweise in der vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen Publikation „Sicherer Einsatz von digitalen Telekommunikationsanlagen“, auf die schon in Kapitel 5.1 hingewiesen wurde, sollten ebenfalls berücksichtigt werden.

7.1 Telekommunikationsanlagen

7.1.1 Personenbezogene Daten

In Telekommunikationsanlagen werden im Regelfall zwei Arten personenbezogener Daten gespeichert und verarbeitet:

- Anschlussdaten

  Für jeden Anschluss (Telefon, Telefax usw.) können administrative Anschlussdaten gespeichert werden, z.B. Name des Anschlussinhabers, Art der Berechtigung, Kurzwahlziele (oft gewählte private und dienstliche Telefonnummern), Geheimnummer des elektronischen Telefonschlosses, zuletzt gewählte Verbindung usw. Diese Daten werden überwiegend von einem Systemverwalter - meist Mitarbeiter der Hausverwaltung - am Betriebsterminal eingegeben und gegebenenfalls geändert.

- Verbindungsdaten

  Für jede abgehende Verbindung wird automatisch ein Datensatz gespeichert, der neben der Rufnummer des Anrufers und des Angerufenen, auch Angaben über Zeitpunkt, Dauer und Art der Verbindung (Telefon, Telefax usw.) enthalten kann. Meist enthalten die Telekommunikationsanlagen bereits in der Erstausstattung Programme, die eine vielfache Auswertung dieser Verbindungsdaten gestatten. So können nicht nur etwa Listen zur Abrechnung der Privatgespräche erstellt werden, sondern die Verbindungsdaten können auch zur Erstellung von „Hitlisten“ benutzt werden (Wer hat am häufigsten telefoniert und/oder die längsten und/oder teuersten Gespräche geführt?). Die möglichen Programme sollten

  - vollständig dokumentiert und
  - nur in dem für den festgelegten Zweck erforderlichen Umfang gespeichert sein.

7.1.2 Zulässigkeit der Datenverarbeitung

Über die in den Kapiteln 2 bis 4 behandelten Datenschutzvorschriften hinaus sind in Behörden wesentlich die Bestimmungen zu beachten, die das Verhältnis zwischen Bediensteten und Dienstherrn regeln. Insbesondere sind dies die „Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Bundesverwaltung (Dienstanschlussvorschriften - DAV -)“ des Bundesministeriums der Finanzen sowie die einschlägigen Vereinbarungen zwischen Dienstherrn und Bediensteten, in der Regel in Form von Dienstvereinbarungen. Aus Sicht des Datenschutzes können nur solche Datenerhebungen und -verarbeitungen als erforderlich und somit zulässig angesehen werden, die von diesen Vorschriften gefordert werden; weitergehende Erhebungen und Verarbeitungen können nur mit Einwilligung der Betroffenen erfolgen.

7.1.3 Dienstanschlussvorschriften (DAV)

Es ist darauf zu achten, dass die zur Erfüllung der DAV erforderlichen Leistungsmerkmale der Telekommunikationsanlage nicht nur im Prospekt stehen, sondern vom Lieferanten auch vertraglich zugesichert werden. Dies gilt insbesondere für die DAV-Vorgaben, bestimmte Angaben in den Verbindungsdatensätzen vor der Speicherung zu unterdrücken (z.B. Zeitpunkt des Gespräches, letzte Ziffern der Zielrufnummern usw.). Verboten ist danach nicht nur der Ausdruck der fraglichen Daten etwa auf einem Einzelverbindungsnachweis. Die Daten dürfen auch nicht in der Datenbank der TK-Anlage gespeichert werden. Außerdem ist darauf zu achten, dass eine fristgerechte Löschung möglich ist.

Aufgrund der bisherigen Erfahrung wird dringend empfohlen, diese Punkte vor der Auftragserteilung mit dem Lieferanten zu klären.

7.1.4 Telekommunikations-Datenschutzverordnung (TDSV)

Wer geschäftsmäßig Telekommunikationsdienste erbringt, muss auch die Regelungen der TDSV beachten. Dies trifft auch für Behörden zu, die ihren Mitarbeitern privates Telefonieren gestatten. In der TDSV werden jedoch in vielen Punkten Ausnahmen für die Anbieter geschlossener Benutzergruppen gemacht.

Da die Regelungen in den DAV meist enger gefasst sind als in der TDSV, gibt es in der Praxis wenig zusätzlich zu beachten.

7.1.5 Mitwirkung der Personalvertretung

Da die Verbindungsdaten geeignet sind, für eine Verhaltens- oder Leistungskontrolle der Bediensteten verwendet zu werden, ist bereits vor der Beschaffung einer Telekommunikationsanlage der Personalrat (oder Betriebsrat) über die Einzelheiten der geplanten Verarbeitungen und Nutzungen zu informieren. Nur auf diesem Wege kann er seine Rechte nach dem Bundespersonalvertretungs- (bzw. Betriebsverfassungs)-gesetz wahrnehmen.

7.1.6 Dienstliche Verbindungen

Eine Vollspeicherung, d. h. eine Speicherung aller Verbindungsdaten einschl. der vollständigen Rufnummer des Angerufenen der Dienstgespräche und -verbindungen ist nur zulässig, wenn diese Daten für eine Kontrolle der durchgeführten Verbindungen im Rahmen einer Fach- oder Dienstaufsicht oder für eine Datenschutzkontrolle benötigt werden. Die Daten dürfen nur für diese Zwecke verwendet und nicht mit anderen automatisierten Personaldateien verknüpft werden. Sie dürfen nur den mit der Kontrolle beauftragten Personen zugänglich gemacht werden und sind nach Abschluss der Kontrolle - spätestens nach einer festzulegenden Frist - zu löschen.

7.1.7 Private Verbindungen

Bei Privatgesprächen und -verbindungen ist die Verbindungsdatenspeicherung nur in dem Umfange zulässig, in dem sie zur Überprüfung der vom Dienstherrn bzw. Arbeitgeber erstellten Telefonrechnung der Bediensteten erforderlich ist und eine Dienstvereinbarung dies bestimmt. Für die Rufnummer des Angerufenen ist dabei in der Regel die Ortsnetzkennzahl ausreichend. Wenn mehr gespeichert werden soll, muss die Anschlussnummer schon bei der Speicherung soweit gekürzt werden, dass eine Identifizierung des Angerufenen nicht mehr möglich ist, also etwa um die letzten drei Ziffern. Daten über Privatgespräche dürfen nur zum Nachweis der Gespräche für den Betroffenen sowie zur Abrechnung der Gebühren verwendet werden. Entsprechend den Regelungen der DAV darf nur auf Verlangen des Bediensteten ein Ausdruck der einzelnen Verbindungsdaten hinsichtlich der Privatgespräche erstellt

und nur diesem zugeleitet werden. Die Verbindungsdaten sind zu löschen, sobald die Gebühren ohne Vorbehalt bezahlt worden sind.

7.1.8 Datensicherung

Die gespeicherten personenbezogenen Daten - insbesondere die Verbindungsdaten - sind gegen unbefugte Einsichtnahme und Veränderung technisch und organisatorisch zu sichern. Das Betriebsterminal sollte nach Möglichkeit nur dem Systemverwalter zugänglich sein. Es sollte, möglichst schriftlich, festgelegt werden, wer die TK-Anlage administrieren und ggf. einem Techniker für Wartungsarbeiten den Zugang zur TK-Anlage gewähren darf.
Die Berechtigung, Daten einzugeben, zu löschen oder zu verändern, ist auf den Systemverwalter zu begrenzen und durch ein individuelles Passwort abzusichern; für den Vertretungsfall kann dieses im versiegelten Umschlag aufbewahrt werden.

Oft sind mehrere „User“ bzw. Berechtigungsklassen - z.B. „Betreiber“ (= Behörde) und „Wartung“ - eingerichtet, für die unterschiedliche Passwörter mit unterschiedlichen Berechtigungen bestehen müssen. Entsprechende vollständige Erläuterungen sollten stets vom Hersteller mitgeliefert werden. Anzahl und Berechtigungsumfang der Passwörter sollten auf das Unerlässliche beschränkt werden: Im Regelfall reichen hierfür zwei Passwörter aus, wobei das eine dem Betreiber (mit seinen besonderen Zugriffsmöglichkeiten - auch auf personenbezogene Daten), das andere der Wartungsfirma zugeordnet ist. Auch letzteres sollte durch die Behörde festgelegt werden, da zu berücksichtigen ist, dass viele Hersteller für ihre Wartungsorganisation ein einheitliches, oft bundesweit geltendes Passwort eingerichtet haben.

7.1.9 Wartung, Fernwartung

Fernwartung sollte nur dann zugelassen werden, wenn sichergestellt ist, dass

1. ein Zugriff durch das Fernwartungszentrum auf die Telekommunikationsanlage auch im Einzelfall nur unter Mitwirkung des Systemverwalters (z.B. durch Betätigen eines Schalters, Freigabe am Betriebsterminal usw.) möglich ist und

2. bei einem solchen Zugriff keine Möglichkeit besteht, personenbezogene Daten der Behörde einzusehen, zu ändern oder zu kopieren. Die Lieferfirma sollte

daher die betreffenden Programme schriftlich erläutern und den Nichtzugriff auf personenbezogene Daten vertraglich bestätigen.

Programme, bei denen der Zugriff auf personenbezogene Daten - insbesondere die Verbindungsdaten - unerlässlich ist, dürfen nur am Betriebsterminal und ebenfalls unter Mitwirkung des Systemverwalters im Einzelfall zu starten sein.

7.1.10 Leistungsmerkmale

Einige Leistungsmerkmale von TK-Anlagen sind geeignet, Gespräche oder Räume abzuhören (siehe 5.1.6 ff). Hier wird empfohlen, sich vor Beschaffung einer Anlage eine Übersicht über die Leistungsmerkmale zu machen und sich schriftlich zusichern zu lassen, dass nicht benötigte kritische Leistungsmerkmale sicher zu deaktivieren sind.

7.2 Telefax

7.2.1 Hinweise zum Datenschutz bei Telefaxübermittlungen

7.2.1.1 Organisatorische Regelungen

Die Nutzung des Telefaxgerätes bzw. der Telefaxanlage sollte durch Dienstanweisung geregelt werden. Dabei sollten insbesondere die grundsätzlichen Voraussetzungen für eine Nutzung, die erforderlichen Sicherheitsvorkehrungen sowie die Verantwortlichkeiten festgelegt werden.

7.2.1.2 Fernmeldegeheimnis

Nach § 85 TKG ist jeder, der „geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt," zur Wahrung des Fernmeldegeheimnisses (siehe 4.2) verpflichtet. Dies gilt auch z. B. für Bedienstete, die ein eingegangenes Telefax dem Gerät entnehmen, um es dem Empfänger zuzuleiten oder die Sende-/Empfangsprotokolle (siehe 7.2.1.3) ausdrucken lassen und verwalten. Die Bediensteten sollten auf die Bedeutung des Fernmeldegeheimnisses, insbesondere die Folgen eines Verstoßes hingewiesen werden.

7.2.1.3 Sende-/Empfangsprotokolle

Telefaxgeräte erzeugen automatisch und/oder auf Wunsch Sende-/Empfangs-protokolle, die bei jedem Vorgang unter anderem Zeitpunkt der Sendung bzw. des Empfangs und die Anschlusskennung der anderen Station enthalten. Diese Daten unterliegen dem besonderen Schutz des Fernmeldegeheimnisses. Die Sende-/Empfangsprotokolle müssen daher entsprechend sorgfältig behandelt werden: Ein Ausdruck durch Unbefugte sollte verhindert, jedenfalls verboten werden; die Einsichtnahme sollte geregelt, die Protokolle müssen sorgfältig und gesichert aufbewahrt werden.

7.2.1.4 Kenntnisnahme durch Unbefugte

Weil Telefaxsendungen beim erreichten Empfänger offen ankommen, ist bei der Versendung besondere Sorgfalt geboten. Vor der Absendung muss deshalb die Gültigkeit der bekannten Anschlussnummer gewährleistet sein. Dabei ist stets zu berücksichtigen, dass eine Telefaxsendung ebenso wie ein Telefongespräch unter Umständen von Unbefugten „abgehört“ werden kann.

- Anschlusskennung des Empfängers

  Durch Falschwahl sowohl beim Absender als auch im Übertragungsnetz des Telekommunikationsunternehmens kann es dazu kommen, dass ein anderer als der gewünschte Anschluss erreicht wird. Zudem kann sich, da freigewordene Anschlussnummern durch die Unternehmen wieder neu vergeben werden, hinter einer bekannten und auch richtig angewählten Anschlussnummer unerwartet ein anderer Partner verbergen. Bei jeder Sendung ist deshalb zu überprüfen, ob auch tatsächlich der richtige Anschluss/Partner erreicht wird: Nahezu jedes Gerät sendet, wenn es von einem anderen Gerät aus angewählt wird, die eigene Anschlusskennung an dieses zurück. Sie besteht aus einem numerischen Teil, z. B. „49 228 81995550“ und im allgemeinen einem Textteil, z. B. „Bundesdatenschutz, Bonn “. Bei Absendung eines Telefax sollte daher stets die Rücksendung der Kennung des angewählten Gerätes abgewartet und diese überprüft werden. Bei fehlender Übereinstimmung sollte im Zweifelsfall die Sendung sofort abgebrochen werden (siehe 5.5).

- Zeitversetzte Sendungen

Bei Sendungen ins Ausland ist die Ortszeit zu überprüfen. Es ist je nach Art des Inhalts sicherzustellen, dass ein Telefax dort nicht außerhalb der Dienstzeit ankommt und somit durch Unbefugte Einsicht genommen werden könnte. Dieser Gesichtspunkt ist auch im Inland dann zu beachten, wenn ein Telefax nicht sofort abgesandt, sondern von der Möglichkeit der zeitversetzten Sendung Gebrauch gemacht wird.

- Anrufumleitung, -weiterschaltung

  Für Telefaxgeräte, die in Telekommunikationsanlagen eingesetzt sind, kann - soweit vorhanden - die Möglichkeit der Anrufumleitung und -weiterschaltung genutzt werden. Dies kann dazu führen, dass eine Sendung bei einem (anderen als dem angewählten) Empfangsgerät ankommt, das in einem fachlich unzuständigen Bereich aufgestellt ist. Dadurch könnte es zu einer datenschutzrechtlich unzulässigen Übermittlung kommen. Dieses Risiko kann durch Überprüfung der rückgesendeten Kennung verringert werden.

- Besonders schutzbedürftige Daten

  Wegen der bestehenden Risiken sollten besonders schutzbedürftige Daten, insbesondere solche, die sich auf
  - strafbare Handlungen,
  - Ordnungswidrigkeiten,
  - religiöse oder politische Anschauungen sowie
  - bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse

  beziehen, nur dann per Telefax übermittelt werden, wenn dies von der Eilbedürftigkeit her geboten und durch besondere Vorkehrungen sichergestellt ist, dass die Sendung (nur) dem Richtigen zugeht. Neben der Beachtung dieser Hinweise ist es geboten, unmittelbar vor der Sendung eine telefonische Vereinbarung möglichst auch über persönliche Entgegennahme der Sendung zu treffen.

7.2.1.5 Dokumentation, Vollständigkeit

Jeder Sendung sollte - soweit technisch möglich - ein Vorblatt vorangefügt werden, welches Absender, dessen Telefax- und Telefonnummer (für Rückrufe) sowie die

Gesamtanzahl der gesendeten Seiten ausweist. Es sollte möglichst für jede einzelne Sendung ein Sendeprotokoll erzeugt und dies dem Vorgang beigefügt werden. Soweit das Gerät eine gesendete Seite durch einen Verifikationsstempel als solche kennzeichnet, sollte die Funktionsfähigkeit dieser Vorrichtung sichergestellt sein.

7.2.1.6 Erhalt der Verfügbarkeit

Bei Ausfall der Netzstromversorgung können die Speicherinhalte des Gerätes (teilweise) gelöscht werden. Dadurch können - sofern vorhanden - Seitenspeicher (für Gruppensendungen usw.) oder Ziel- und Gruppenwahlnummern gelöscht oder unrichtig werden. Dies ist von Zeit zu Zeit, bei bekannt gewordenem Netzausfall in jedem Fall, zu überprüfen.

7.2.1.7 Räumliche Unterbringung

Telefaxgeräte sollten nach Möglichkeit in Räumen untergebracht werden, die ausreichend gesichert sind. Ansonsten sollte anderweitig sichergestellt werden, dass eine Telefaxsendung nicht unbeobachtet ankommt und von Unbefugten entnommen oder eingesehen werden kann.

7.2.2 Merkblatt für Bundesbehörden zum Datenschutz bei Telefax

1. Sie tragen die Verantwortung für die durch Sie übermittelten personenbezogenen Daten; prüfen Sie daher genau deren Sensibilität.

2. Beachten Sie die für Ihre Behörde/Dienststelle geltenden Anweisungen für das Senden und Empfangen von Telefaxen.

3. Nutzen Sie nach Möglichkeit alle der Sicherheit dienenden Einrichtungen des Gerätes, insbesondere die Anzeige des erreichten Gerätes.

4. Vergewissern Sie sich vor einer Sendung, ob der Adressat noch unter der Ihnen bekannten Anschlussnummer erreichbar ist.

5. Verständigen Sie sich vor der Absendung besonders sensibler Daten mit dem Adressaten über den konkreten Zeitpunkt der Übermittlung!

6. Gewährleisten Sie - möglichst durch persönliche Anwesenheit am Gerät - während der Übertragung von Dokumenten mit personenbezogenen Daten, dass kein Unbefugter in diese Einsicht nehmen kann.

7. Verständigen Sie sich nach Empfang einer Sendung mit Ihrem Partner über aufgetretene Mängel und ggf. deren Behebung.

8. Erleichtern Sie sich und Ihren Partnern die Nachweisführung:
   - Vorblatt der Behörde/Dienststelle benutzen,
   - Aussagekräftiges „Logo“ vorprogrammieren,
   - Blattnummerierung der Kopien,
   - Originale mit Verifikationsstempel versehen,
   - Journalfunktion nutzen.

9. Faxübertragungen sind „abhörbar“: Was am Telefon nicht gesagt werden darf, darf auch nicht gefaxt werden!

10. Beachten Sie bei der Nutzung von Faxservern neben den erweiterten Möglichkeiten auch die damit verbundenen Risiken; verständigen Sie sich darüber mit Ihrem Datenschutzbeauftragten.

7.3 Anrufbeantworter mit Fernbedienung

Die meisten der heute angebotenen telefonischen Anrufbeantworter weisen die Möglichkeit der Fernabfrage der aufgezeichneten Telefonate, zum Teil auch der Fernbedienung aller Gerätefunktionen, insbesondere der Raumüberwachungsfunktion, auf. Die Fernabfrage über einen beliebigen Telefonanschluss erfolgt mittels eines Codes im sogenannten Mehrfrequenzwahlverfahren (MFV) durch Eingabe von Ziffern- oder Zeichenkombinationen am Telefonendgerät.

Problematisch ist, dass bei einem Teil der angebotenen Geräte der Schutz gegen unbefugte Abfrage mangelhaft ist. So ist es beispielsweise möglich, durch eine Vielzahl aufeinanderfolgender Versuche die Codierung „durch Probieren“ in Erfahrung zu bringen. Technisch versierte Telekommunikationsteilnehmer sind auch in der Lage, durch ein Programm die Codierung zu ermitteln. Dem Bundesbeauftragten für den Datenschutz wurde zudem berichtet, dass einige der Geräte über eine „Notsicherung“ für den Fall verfügen, dass der Berechtigte den richtigen Code vergessen hat oder der Code nach einem Stromausfall gelöscht worden ist. In diesem Fall muss dann lediglich die Codierung „0 0 0 0“ neu eingestellt werden. Auch eine voreingestellte, nicht veränderbare Codierung muss als Sicherheitsrisiko angesehen werden, vor allem dann, wenn sie - was tatsächlich vorgekommen ist - mit einem Aufkleber auf der Unterseite des Gerätes angebracht und für jedermann ersichtlich ist.

Der Bundesbeauftragte für den Datenschutz empfiehlt allen Stellen, bei denen Anrufbeantworter mit Fernabfrage im Einsatz sind, folgende Sicherheitshinweise zu beachten:

1. Ändern Sie umgehend, soweit noch nicht geschehen, die werksseitig eingestellte Codierung.

2. Stellen Sie den Anrufbeantworter - insbesondere, wenn er über eine Raumüberwachungsfunktion verfügt - nur in solchen Diensträumen auf, in denen keine schutzbedürftigen dienstlichen Gespräche stattfinden.

3. Ändern Sie in regelmäßigen Abständen die Codierung.

4. Verzichten Sie auf Trivialcodierungen, wie z.B. 007, oder „Monatsschlüssel“, z.B. 003.

5. Prüfen Sie, ob Ihr Gerät über die o. g. „Notfallsicherung“ verfügt; sie stellt ein untragbares Sicherheitsrisiko dar!

6. Weisen Sie bitte im Ansagetext darauf hin, dass die gespeicherte Nachricht eventuell Unbefugten zugänglich ist.

7. Klären Sie ggf. Ihre Mitarbeiter über die Mithörmöglichkeiten der Raumüberwachungsfunktion auf.

8. Achten Sie beim Abhören der Nachrichten auf Unregelmäßigkeiten bzw. auf Signale, die auf einen unbefugten Abhörer hindeuten könnten.

9. Achten Sie bei Neubeschaffung darauf, dass das Gerät sowohl über eine jederzeit veränderbare, mindestens vierstellige Codierung als auch über die Möglichkeit verfügt, nach max. drei Fehlversuchen die Verbindung zu unterbrechen.

Anhang 1

Gesetzes- und Verordnungstexte

Übersicht:

Hinweis:
Die in Anhang 1 abgedruckten Rechtsvorschriften erheben keinen Anspruch auf Aktualität, sachliche Korrektheit oder Vollständigkeit. Es wird ausdrücklich darauf hingewiesen, dass Gesetze und Verordnungen nur in ihrer jeweils aktuellsten Fassung, entsprechend dem im Bundesgesetzblatt veröffentlichten Wortlaut, gültig sind und Anwendung finden.

I.1 Artikel 10 Grundgesetz

Art. 10 [Brief-, Post- und Fernmeldegeheimnis]

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

I.2 Auszug aus dem Bundesdatenschutzgesetz (BDSG)

Hinweis:
Es handelt sich um einen nichtamtlichen BDSG-Text unter Berücksichtigung des am 23. Mai 2001 in Kraft getretenen Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze vom 18.05. 2001 (BGBl. I S. 904).

§ 1

Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des

Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zwecke des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

§ 2

Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3

Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,
2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

§ 3a

Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 4

Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

   und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a

Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4b

Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,
2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder
3. der Organe und Einrichtungen der Europäischen Gemeinschaften

gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

(2) Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend. Die
Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die

Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.

§ 4c

Ausnahmen

(1) Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern

1. der Betroffene seine Einwilligung gegeben hat,
2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.

(2) Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Bei den Post- und Telekommunikationsunternehmen ist der Bundesbeauftragte für den Datenschutz zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.

(3) Die Länder teilen dem Bund die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.

§ 4d

Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung oder

2. zum Zweck der anonymisierten Übermittlung

gespeichert werden.

(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der

Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz zu wenden.

§ 4e

Inhalt der Meldepflicht

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

§ 4f

Beauftragter für den Datenschutz

(1) Öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für nicht öffentliche Stellen, die höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erheben, verarbeiten oder nutzen, haben sie unabhängig von der Anzahl der Arbeitnehmer einen Beauftragten für den Datenschutz zu bestellen.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht öffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nicht öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(5) Die öffentlichen und nicht öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm

insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

§ 4g

Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Im Fall des § 4d Abs. 2 macht der Beauftragte für den Datenschutz die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar. Im Fall des § 4d Abs. 3 gilt Satz 2 entsprechend für die verantwortliche Stelle.

(3) Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde.

§ 5

Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht öffentlichen Stellen

beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6

Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

X

X

X

§ 7

Schadensersatz

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

X

X

X

§ 9

Technische und organisatorische Maßnahmen

Öffentliche und nicht öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 9a

Datenschutzaudit

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

X

X

X

§ 11

Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1, Abs. 3 und 4 sowie § 44 Abs. 1 Nr. 2, 5, 6 und 7 und Abs. 2 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,

   b) nicht öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

   die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f , 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht aus-geschlossen werden kann.

X

X

X

§ 21

Anrufung des Bundesbeauftragten für den Datenschutz

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

§ 22

Wahl des Bundesbeauftragten für den Datenschutz

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muss bei seiner Wahl das 35. Lebensjahr vollendet haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(2) Der Bundesbeauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

> "Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe."

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.
(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.

(5) Der Bundesbeauftragte wird beim Bundesministerium des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministeriums des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministeriums des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

X

X

X

§ 24

Kontrolle durch den Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs, und
2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 Grundgesetz wird insoweit eingeschränkt. Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 Grundgesetz unterliegen, unterliegen nicht der Kontrolle durch den Bundesbeauftragten, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch den Bundesbeauftragten unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25

Beanstandungen durch den Bundesbeauftragten für den Datenschutz

(1) Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,
4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§ 26

Weitere Aufgaben des Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. § 38 Abs. 1 Satz 3 und 4 gilt entsprechend.

X

X

X

§ 33

Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der

Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,
4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,
5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
7. die Daten für eigene Zwecke gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder
   b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder
8. die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder
   b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Abs. 2 Nr. 1 Buchstabe b)

   und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

§ 34

Auskunft an den Betroffenen

(1) Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. In diesem Fall ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.

(2) Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie weder in einer automatisierten Verarbeitung noch in einer nicht automatisierten Datei gespeichert sind. Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.

(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(5) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, dass die Daten zu berichtigen oder unter der Voraussetzung des § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(6) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Er ist hierauf in geeigneter Weise hinzuweisen.

§ 35

Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,
2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Falle des Absatzes 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu

Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.
(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1 es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

X

X

X

§ 43

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig
oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,
7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,
8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,
10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder
11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
6. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 2 Satz 3 die in § 40 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu fünfhunderttausend Deutsche Mark geahndet werden.

§ 44

Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde.

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

II.1 Auszug aus dem Telekommunikationsgesetz (TKG)

§ 1
Zweck des Gesetzes

Zweck dieses Gesetzes ist es, durch Regulierung im Bereich der Telekommunikation den Wettbewerb zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten sowie eine Frequenzordnung festzulegen.

§ 2
Regulierung

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

(2) Ziele der Regulierung sind:

1. die Wahrung der Interessen der Nutzer auf dem Gebiet der Telekommunikation und des Funkwesens sowie die Wahrung des Fernmeldegeheimnisses,

2. die Sicherstellung eines chancengleichen und funktionsfähigen Wettbewerbs, auch in der Fläche, auf den Märkten der Telekommunikation,

3. die Sicherstellung einer flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen (Universaldienstleistungen) zu erschwinglichen Preisen,

4. die Förderung von Telekommunikationsdiensten bei öffentlichen Einrichtungen,

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

6. die Wahrung der Interessen der öffentlichen Sicherheit.

(3) Die Vorschriften des Gesetzes gegen Wettbewerbsbeschränkungen bleiben unberührt.

(4) Die hoheitlichen Rechte des Bundesministers der Verteidigung bleiben unberührt.

§ 3
Begriffsbestimmungen

Im Sinne dieses Gesetzes

1. ist "Betreiben von Übertragungswegen" Ausüben der rechtlichen und tatsächlichen Kontrolle (Funktionsherrschaft) über die Gesamtheit der Funktionen, die zur Realisierung der Informationsübertragung auf Übertragungswegen unabdingbar erbracht werden müssen,

2. ist "Betreiben von Telekommunikationsnetzen" Ausüben der rechtlichen und tatsächlichen Kontrolle (Funktionsherrschaft) über die Gesamtheit der Funktionen, die zur Erbringung von Telekommunikationsdienstleistungen oder nichtgewerblichen Telekommunikationszwecken über Telekommunikationsnetze unabdingbar zur Verfügung gestellt werden müssen; dies gilt auch dann, wenn im Rahmen des Telekommunikationsnetzes Übertragungswege zum Einsatz kommen, die im Eigentum Dritter stehen,

3. sind "Endeinrichtungen" Einrichtungen, die unmittelbar an die Abschlusseinrichtung eines Telekommunikationsnetzes angeschlossen werden sollen oder die mit einem Telekommunikationsnetz zusammenarbeiten und dabei unmittelbar oder mittelbar an die Abschlusseinrichtung eines Telekommunikationsnetzes angeschlossen werden sollen,

4. sind "Funkanlagen" elektrische Sende- oder Empfangseinrichtungen, zwischen denen die Informationsübertragung ohne Verbindungsleitungen stattfinden kann,

5. ist "geschäftsmäßiges Erbringen von Telekommunikationsdiensten" das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht,

6. ist "Grundstück" ein im Grundbuch als selbständiges Grundstück eingetragener Teil der Erdoberfläche oder ein Teil der Erdoberfläche, der durch die Art seiner wirtschaftlichen Verwendung oder nach seiner äußeren Erscheinung eine Einheit bildet, und zwar auch dann, wenn es sich im liegenschaftsrechtlichen Sinn um mehrere Grundstücke handelt. Straßen- und Schienennetze werden nicht als einheitliches Grundstück betrachtet,

7. ist "Lizenz" die Erlaubnis zum Angebot bestimmter Telekommunikationsdienstleistungen für die Öffentlichkeit,

8. sind "Mobilfunkdienstleistungen" Telekommunikationsdienstleistungen, die für die mobile Nutzung bestimmt sind,

9. ist "Netzzugang" die physische und logische Verbindung von Endeinrichtungen oder sonstigen Einrichtungen mit einem Telekommunikationsnetz oder Teilen desselben sowie die physische und logische Verbindung eines Telekommunikationsnetzes mit einem anderen Telekommunikationsnetz oder Teilen desselben zum Zwecke des Zugriffs auf Funktionen dieses Telekommunikationsnetzes oder auf die darüber erbrachten Telekommunikationsdienstleistungen,

10. sind "Nummern" Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen,

11. sind "Nutzer" Nachfrager nach Telekommunikationsdienstleistungen,

12. ist "öffentliches Telekommunikationsnetz" die Gesamtheit der technischen Einrichtungen (Übertragungswege, Vermittlungseinrichtungen und sonstige Einrichtungen, die zur Gewährleistung eines ordnungsgemäßen Betriebs des Telekommunikationsnetzes unerlässlich sind), an die über Abschlusseinrichtungen Endeinrichtungen angeschlossen werden und die zur Erbringung von Telekommunikationsdienstleistungen für die Öffentlichkeit dient,

13. sind "Regulierung" die Maßnahmen, die zur Erreichung der in § 2 Abs. 2 genannten Ziele ergriffen werden und durch die das Verhalten von Telekommunikationsunternehmen beim Angebot von Telekommunikationsdienstleistungen, von Endeinrichtungen oder von Funkanlagen geregelt werden, sowie die Maßnahmen, die zur Sicherstellung einer effizienten und störungsfreien Nutzung von Frequenzen ergriffen werden,

14. sind "Satellitenfunkdienstleistungen" Telekommunikationsdienstleistungen, die unter Zuhilfenahme von Satellitenfunkanlagen erbracht werden,

15. ist "Sprachtelefondienst" die gewerbliche Bereitstellung für die Öffentlichkeit des direkten Transports und der Vermittlung von Sprache in Echtzeit von und zu den Netzabschlusspunkten des öffentlichen, vermittelnden Netzes, wobei jeder

Benutzer das an solch einem Netzabschlusspunkt angeschlossene Endgerät zur Kommunikation mit einem anderen Netzabschlusspunkt verwenden kann,

16. ist "Telekommunikation" der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen,

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

18. sind "Telekommunikationsdienstleistungen" das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte,

19. sind "Telekommunikationsdienstleistungen für die Öffentlichkeit" das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für beliebige natürliche oder juristische Personen und nicht lediglich für die Teilnehmer geschlossener Benutzergruppen,

20. sind "Telekommunikationslinien" unter- oder oberirdisch geführte Telekommunikationskabelanlagen einschließlich ihrer zugehörigen Schalt- und Verzweigungseinrichtungen, Masten und Unterstützungen, Kabelschächte und Kabelkanalrohre,

21. ist "Telekommunikationsnetz" die Gesamtheit der technischen Einrichtungen (Übertragungswege, Vermittlungseinrichtungen und sonstige Einrichtungen, die zur Gewährleistung eines ordnungsgemäßen Betriebs des Telekommunikationsnetzes unerlässlich sind), die zur Erbringung von Telekommunikationsdienstleistungen oder zu nichtgewerblichen Telekommunikationszwecken dient,

22. sind "Übertragungswege" Telekommunikationsanlagen in Form von Kabel- oder Funkverbindungen mit ihren übertragungstechnischen Einrichtungen als Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen mit einem bestimmten Informationsdurchsatzvermögen (Bandbreite oder Bitrate) einschließlich ihrer Abschlusseinrichtungen,

23. ist "Verbindungsnetz" ein Telekommunikationsnetz, das keine Teilnehmeranschlüsse aufweist und Teilnehmernetze miteinander verbindet,

24. ist "Zusammenschaltung" derjenige Netzzugang, der die physische und logische Verbindung von Telekommunikationsnetzen herstellt, um Nutzern, die an verschiedenen Telekommunikationsnetzen angeschaltet sind, die mittelbare oder unmittelbare Kommunikation zu ermöglichen.

§ 4
Anzeigepflicht

Jeder, der Telekommunikationsdienstleistungen erbringt, muss die Aufnahme, Änderung und Beendigung des Betriebes innerhalb eines Monats bei der Regulierungsbehörde schriftlich anzeigen. Die Regulierungsbehörde veröffentlicht regelmäßig den wesentlichen Inhalt der Anzeigen.

§ 5
Berichtspflichten

Jeder, der Telekommunikationsdienstleistungen erbringt, ist verpflichtet, auf Verlangen der Regulierungsbehörde dieser Berichte zur Verfügung zu stellen, die sie als nationale Regulierungsbehörde zur Erfüllung ihrer Berichtspflichten gegenüber der Europäischen Kommission auf Grund von Richtlinien und Empfehlungen, die nach Artikel 6 der Richtlinie 90/387/EWG des Rates vom 28. Juni 1990 zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provision – ONP) (ABl. EG Nr. L 192 S. 1) sowie nach Artikel 90 Abs. 3 des Vertrages zur Gründung der Europäischen Gemeinschaft erlassen werden, benötigt.

§ 6
Lizenzpflichtiger Bereich

(1) Einer Lizenz bedarf, wer

1. Übertragungswege betreibt, die die Grenze eines Grundstücks überschreiten und für Telekommunikationsdienstleistungen für die Öffentlichkeit genutzt werden,

2. Sprachtelefondienst auf der Basis selbst betriebener Telekommunikationsnetze anbietet.

(2) Die nach Absatz 1 erforderlichen Lizenzen werden in folgende Lizenzklassen eingeteilt:

1. Lizenzen zum Betreiben von Übertragungswegen

   a) für Mobilfunkdienstleistungen für die Öffentlichkeit durch den Lizenznehmer oder andere (Lizenzklasse 1: Mobilfunklizenz),

   b) für Satellitenfunkdienstleistungen für die Öffentlichkeit durch den Lizenznehmer oder andere (Lizenzklasse 2: Satellitenfunklizenz),

   c) für Telekommunikationsdienstleistungen für die Öffentlichkeit durch den Lizenznehmer oder andere, für deren Angebot nicht die Lizenzklasse 1 oder 2 bestimmt ist (Lizenzklasse 3),

2. Lizenzen für Sprachtelefondienst auf der Basis selbst betriebener Telekommunikationsnetze (Lizenzklasse 4). Diese Lizenzklasse schließt nicht das Recht zum Betreiben von Übertragungswegen ein.

(3) Es wird vermutet, dass das Betreiben von Übertragungswegen, die von Dritten genutzt werden, eine Telekommunikationsdienstleistung für die Öffentlichkeit darstellt.

(4) Die Regulierungsbehörde kann auf Antrag Lizenzen der Lizenzklassen 1 bis 4 auch in einer Lizenz zusammengefasst erteilen. Dabei ist sie an den vorgegebenen Rahmen des Absatzes 1 gebunden.

§ 7
Internationaler Status

Lizenznehmer, die internationale Telekommunikationsdienstleistungen erbringen oder im Rahmen ihres Angebots Funkanlagen betreiben, die schädliche Störungen bei Funkdiensten anderer Länder verursachen können, sind anerkannte Betriebsunternehmen im Sinne der Konstitution und der Konvention der Internationalen Fernmeldeunion.

§ 8

Lizenzerteilung

(1) Die Lizenz wird auf schriftlichen Antrag von der Regulierungsbehörde schriftlich erteilt. Im Lizenzantrag ist das Gebiet zu bezeichnen, in dem die lizenzpflichtige Tätigkeit ausgeübt werden soll. Die Regulierungsbehörde soll über Lizenzanträge innerhalb von sechs Wochen entscheiden.

(2) Bei der Lizenzerteilung sind die Regulierungsziele nach § 2 Abs. 2 zu beachten. Zur Sicherstellung der Regulierungsziele nach § 2 Abs. 2 können der Lizenz Nebenbestimmungen, auch nach Erteilung der Lizenz, beigefügt werden. Sind die Voraussetzungen für eine Nebenbestimmung entfallen, so hat die Regulierungsbehörde diese auf Antrag des Lizenznehmers aufzuheben.

(3) Eine beantragte Lizenz ist zu versagen, wenn

1. die Regulierungsbehörde über keine nutzbaren Frequenzen verfügt, die dem Antragsteller, der Funkverbindungen betreiben möchte, zugeteilt werden können oder

2. Tatsachen die Annahme rechtfertigen, dass

   a) der Antragsteller nicht die für die Ausübung der beantragten Lizenzrechte erforderliche Zuverlässigkeit, Leistungsfähigkeit und Fachkunde besitzt und damit zu erwarten ist, dass diese Lizenzrechte nicht dauerhaft ausgeübt werden, oder

   b) durch die Lizenzerteilung die öffentliche Sicherheit oder Ordnung gefährdet würde.

Die nach Satz 1 Nr. 2 Buchstabe a erforderliche

1. Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, dass er als Lizenznehmer die Rechtsvorschriften einhalten wird,

2. Leistungsfähigkeit besitzt, wer die Gewähr dafür bietet, dass ihm die für den Aufbau und den Betrieb der zur Ausübung der Lizenzrechte erforderlichen Produktionsmittel zur Verfügung stehen werden,

3. Fachkunde besitzt, wer die Gewähr dafür bietet, dass die bei der Ausübung der Lizenzrechte tätigen Personen über die erforderlichen Kenntnisse, Erfahrungen und Fertigkeiten verfügen werden.

(4) Die Lizenz kann befristet erteilt werden, soweit dieses wegen Knappheit der zur Verfügung stehenden Frequenzen geboten ist.

(5) Zum Betrieb von Übertragungswegen im Rahmen einer Lizenz benötigte Frequenzen werden nach Maßgabe
der §§ 44 bis 48 zugeteilt.

X

X

X

§ 12
Bereitstellen von Teilnehmerdaten

(1) Ein Lizenznehmer, der Sprachkommunikationsdienstleistungen für die Öffentlichkeit anbietet, ist verpflichtet, auf Anforderung Teilnehmerdaten unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen anderen Lizenznehmern, die Sprachkommunikationsdienstleistungen für die Öffentlichkeit anbieten, zum Zwecke der Aufnahme eines Auskunftsdienstes oder der Herausgabe eines Verzeichnisses der Rufnummern der Teilnehmer in kundengerechter Form zugänglich zu machen. Hierfür kann ein Entgelt erhoben werden, das sich an den Kosten der effizienten Bereitstellung orientiert.

(2) Ein Lizenznehmer, der Sprachkommunikationsdienstleistungen für die Öffentlichkeit anbietet, ist darüber hinaus verpflichtet, auf Anforderung Teilnehmerdaten unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen jedem Dritten zum Zwecke der Aufnahme eines Auskunftsdienstes oder der Herausgabe eines Verzeichnisses der Rufnummern der Teilnehmer in kundengerechter Form gegen ein angemessenes Entgelt zugänglich zu machen.

§ 13
Bereitstellen von Notrufmöglichkeiten

(1) Ein Lizenznehmer, der Sprachkommunikationsdienstleistungen für die Öffentlichkeit anbietet, ist verpflichtet, unentgeltlich Notrufmöglichkeiten für jeden Endnutzer bereitzustellen.

(2) Ein Lizenznehmer, der Sprachkommunikationsdienstleistungen für die Öffentlichkeit anbietet, hat auf Antrag des zuständigen Bundeslandes oder eines ermächtigten Notdienstträgers in öffentlichen Telefonstellen zusätzlich Notrufeinrichtungen einzurichten, die es dem Nutzer ermöglichen, durch einfache Handhabung und möglichst unter automatischer Anzeige des Standortes der benutzten Telefonstelle Sprechverbindung mit einer Notrufabfragestelle aufzunehmen. öffentliche Telefonstellen, in denen sich Einrichtungen nach Satz 1 befinden, sind besonders zu kennzeichnen. Für das Bereitstellen und den Betrieb von Notrufeinrichtungen ist vom Antragsteller ein Entgelt zu erheben, das die vollen Kosten deckt.

§ 14
Strukturelle Separierung und getrennte Rechnungsführung

(1) Unternehmen, die auf anderen Märkten als der Telekommunikation über eine marktbeherrschende Stellung nach § 19 des Gesetzes gegen Wettbewerbsbeschränkungen verfügen, müssen Telekommunikationsdienstleistungen in einem oder mehreren rechtlich selbständigen Unternehmen führen.

(2) Unternehmen, die auf einem Markt der Telekommunikation über eine marktbeherrschende Stellung nach § 19 des Gesetzes gegen Wettbewerbsbeschränkungen verfügen, müssen die Nachvollziehbarkeit der finanziellen Beziehungen zwischen Telekommunikationsdienstleistungen im lizenzpflichtigen Bereich zueinander und dieser zu Telekommunikationsdienstleistungen im nicht lizenzpflichtigen Bereich durch Schaffung eines eigenen Rechnungslegungskreises gewährleisten. Dabei kann die Regulierungsbehörde die Gestaltung der internen Rechnungslegung für bestimmte lizenzpflichtige Telekommunikationsdienstleistungen vorgeben.

§ 15
Widerruf der Lizenz

Eine Lizenz kann ganz oder teilweise widerrufen werden, wenn

1. der Lizenznehmer den Verpflichtungen aus seiner Lizenz oder seinen Verpflichtungen nach diesem Gesetz nicht nachkommt, insbesondere gegen das

Fernmeldegeheimnis, datenschutzrechtliche Regelungen oder Strafvorschriften verstößt,

2. in den Fällen des § 9 Abs. 2 beim Lizenznehmer oder demjenigen, dem die Lizenz überlassen wurde, ein Versagungsgrund nach § 8 Abs. 3 Satz 1 Nr. 2 entsteht.

§ 16
Lizenzgebühr

(1) Lizenzen werden gegen Gebühr erteilt. Das Bundesministerium für Post und Telekommunikation wird ermächtigt, im Einvernehmen mit dem Bundesministerium des Innern, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz und dem Bundesministerium für Wirtschaft durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Maßgabe des Verwaltungskostengesetzes die gebührenpflichtigen Tatbestände, die Höhe der Gebühr und die Erstattung von Auslagen zu regeln.

(2) Im Falle des Versteigerungsverfahrens nach § 11 Abs. 4 wird eine Gebühr nach Absatz 1 nur erhoben, soweit sie den Erlös des Versteigerungsverfahrens übersteigt.

X

X

X

§ 40
Anspruch auf Schadenersatz und Unterlassung

Ein Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit, der vorsätzlich oder fahrlässig gegen dieses Gesetz, gegen eine auf Grund dieses Gesetzes erlassene Rechtsverordnung oder gegen eine auf Grund dieses Gesetzes in der Lizenz festgelegte Verpflichtung oder eine Anordnung der Regulierungsbehörde verstößt, ist, sofern die Vorschrift oder die Verpflichtung den Schutz eines Nutzers bezweckt, diesem zum Ersatz des aus dem Verstoß entstandenen Schadens verpflichtet. Er kann von diesem auch auf Unterlassung in Anspruch genommen werden.

§ 41
Kundenschutzverordnung

(1) Die Bundesregierung wird ermächtigt, zum besonderen Schutze der Nutzer, insbesondere der Verbraucher, durch Rechtsverordnung mit Zustimmung des Bundesrates Rahmenvorschriften für die Inanspruchnahme von Telekommunikationsdienstleistungen für die Öffentlichkeit zu erlassen.

(2) In der Rechtsverordnung können insbesondere Regelungen über den Vertragsabschluß, den Gegenstand und die Beendigung der Verträge getroffen und die Rechte und Pflichten der Vertragspartner sowie der sonstigen am Telekommunikationsverkehr Beteiligten festgelegt werden. Dabei sind die Richtlinien zu beachten, die nach Artikel 6 der Richtlinie 90/387/EWG des Rates vom 28. Juni 1990 zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provision – ONP) (ABl. EG Nr. L 192 S. 1) vom Parlament der Europäischen Gemeinschaft und vom Rat erlassen werden, soweit sie die Stellung der Nutzer regeln.

(3) Insbesondere sind Regelungen zu treffen über

1. die Haftung der Anbieter und Schadenersatz- und Unterlassungsansprüche der Nutzer,

2. die Entbündelung von Telekommunikationsdienstleistungen für die Öffentlichkeit im lizenzpflichtigen und im nicht lizenzpflichtigen Bereich sowie die Entbündelung dieser Dienstleistungen untereinander,

3. nähere Bedingungen für die Bereitstellung und Nutzung allgemeiner Netzzugänge nach § 35 Abs. 1; die Bedingungen müssen auf objektiven Maßstäben beruhen, nachvollziehbar sein und einen gleichwertigen Zugang gewährleisten,

4. die Form des Hinweises auf Allgemeine Geschäftsbedingungen und Entgelte und die Möglichkeit ihrer Einbeziehung,

5. Informationspflichten,

6. die bei Angebotsänderungen einzuhaltenden Verfahren und Fristen,

7. besondere Anforderungen für die Rechnungserstellung und für den Nachweis über die Höhe der Entgelte und

8. außergerichtliche Streitbeilegungsverfahren.

§ 42
Rundfunksendeanlagen

Bei der Veräußerung von Sendeanlagen tritt der Erwerber in bestehende Vertragsverhältnisse mit Rundfunkveranstaltern ein.

X
X
X

§ 85
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 verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. 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 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 Fahrzeugs für Seefahrt oder Luftfahrt, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber dem Führer des Fahrzeugs oder seinem Stellvertreter.

§ 86
Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen

Mit einer Funkanlage dürfen Nachrichten, die für die Funkanlage nicht bestimmt sind, nicht abgehört werden. Der Inhalt solcher 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 § 85 besteht, anderen nicht mitgeteilt werden. § 85 Abs. 4 gilt entsprechend. Das Recht, Funkaussendungen zu empfangen, die für die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, sowie das Abhören und die Weitergabe von Nachrichten auf Grund besonderer gesetzlicher Ermächtigung bleiben unberührt.

§ 87
Technische Schutzmaßnahmen

(1) Wer Telekommunikationsanlagen betreibt, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen, hat bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

1. des Fernmeldegeheimnisses und personenbezogener Daten,

2. der programmgesteuerten Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe,

3. gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und

4. von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Angriffe und Einwirkungen von Katastrophen

zu treffen. Dabei ist der Stand der technischen Entwicklung zu berücksichtigen. Die Regulierungsbehörde erstellt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik nach Anhörung von Verbraucherverbänden und von Wirtschaftsverbänden der Hersteller und Betreiber von Telekommunikationsanlagen einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen, um eine nach dem Stand der Technik und internationalen Maßstäben angemessene Standardsicherheit zu erreichen. Dem Bundesbeauftragten für den Datenschutz ist Gelegenheit zur

Stellungnahme zu geben. Der Katalog wird von der Regulierungsbehörde im Bundesanzeiger veröffentlicht. Der für die Schutzmaßnahmen zu erbringende technische und wirtschaftliche Aufwand ist von der Bedeutung der zu schützenden Rechte und der zu sichernden Anlagen für die Allgemeinheit abhängig.

(2) Lizenzpflichtige Betreiber von Telekommunikationsanlagen haben einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,

1. welche Telekommunikationsanlagen eingesetzt und welche Telekommunikationsdienste geschäftsmäßig erbracht werden,

2. von welchen Gefährdungen auszugehen ist und

3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus Absatz 1 getroffen oder geplant sind.

Das Sicherheitskonzept ist der Regulierungsbehörde vorzulegen, verbunden mit einer Erklärung, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder bis zu einem bestimmten Zeitpunkt umgesetzt werden. Stellt die Regulierungsbehörde im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie vom Betreiber deren Beseitigung verlangen.

(3) Das Bundesministerium für Post und Telekommunikation wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, die Erfüllung der Verpflichtungen nach den Absätzen 1 und 2 näher zu regeln. Dabei kann der Kreis der Verpflichteten nach Absatz 1 und das zu fordernde Maß an Schutzvorkehrungen nach den Absätzen 1 und 2 entsprechend der wirtschaftlichen Bedeutung der jeweiligen Telekommunikationsanlage festgelegt werden.

§ 88
Technische Umsetzung von Überwachungsmaßnahmen

(1) Die technischen Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation sind von dem Betreiber der Telekommunikationsanlage auf eigene Kosten zu gestalten und vorzuhalten.

(2) Die technische Gestaltung dieser Einrichtungen bedarf bei Betreibern von Telekommunikationsanlagen, die gesetzlich verpflichtet sind, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, der Genehmigung der Regulierungsbehörde. Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf,

1. die Anforderungen an die Gestaltung der technischen Einrichtungen sowie an die organisatorische Umsetzung von Überwachungsmaßnahmen mittels dieser Einrichtungen und

2. das Genehmigungsverfahren und das Verfahren der Abnahme zu regeln sowie

3. zu bestimmen, bei welchen Telekommunikationsanlagen aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit abweichend von Absatz 1 technische Einrichtungen nicht zu gestalten oder vorzuhalten sind.

Die Rechtsverordnung kann vorsehen, dass in technisch begründeten Ausnahmefällen auf Antrag von der Erfüllung einzelner technischer Anforderungen an die Gestaltung der Einrichtungen abgesehen und mit welchen Nebenbestimmungen die Genehmigung in diesen Fällen versehen werden kann. Der Betrieb einer Telekommunikationsanlage darf erst aufgenommen werden, wenn der Betreiber der Telekommunikationsanlage

1. die in Absatz 1 bezeichneten technischen Einrichtungen nach Maßgabe der Rechtsverordnung nach Satz 2 eingerichtet hat,

2. dies der Regulierungsbehörde schriftlich angezeigt hat und

3. der Regulierungsbehörde im Rahmen der Abnahme unentgeltlich nachgewiesen hat, dass die Genehmigungsvoraussetzungen erfüllt sind.

Die Regulierungsbehörde soll über die Genehmigung binnen sechs Wochen nach Eingang des Antrags und über die Abnahme binnen sechs Wochen nach Eingang der schriftlichen Anzeige nach Satz 4 Nr. 2 entscheiden. Stellt sich nachträglich ein Mangel der Funktionsfähigkeit heraus, hat der Betreiber der Telekommunikationsanlage die Einrichtung unverzüglich nachzubessern.

(3) Telekommunikationsanlagen, mittels derer in das Fernmeldegeheimnis eingegriffen werden soll und die von den gesetzlich berechtigten Stellen betrieben werden, sind im Einvernehmen mit der Regulierungsbehörde technisch zu gestalten.

(4) Jeder Betreiber einer Telekommunikationsanlage, der anderen den Netzzugang zu seiner Telekommunikationsanlage geschäftsmäßig überlässt, ist verpflichtet, den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf deren Anforderung einen Netzzugang für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen unverzüglich und vorrangig bereitzustellen. Die technische Ausgestaltung derartiger Netzzugänge kann in der Rechtsverordnung nach Absatz 2 geregelt werden. Für die Bereitstellung und Nutzung gelten mit Ausnahme besonderer Tarife oder Zuschläge für vorrangige oder vorzeitige Bereitstellung die jeweils für die Allgemeinheit anzuwendenden Tarife. Besondere vertraglich vereinbarte Rabattierungsregelungen bleiben von Satz 3 unberührt.

(5) Die nach den §§ 100a und 100b der Strafprozessordnung verpflichteten Betreiber von Telekommunikationsanlagen haben eine Jahresstatistik über nach diesen Vorschriften durchgeführte Überwachungsmaßnahmen zu erstellen und der Regulierungsbehörde unentgeltlich zur Verfügung zu stellen. Die Ausgestaltung der Statistik im einzelnen kann in der Rechtsverordnung nach Absatz 2 geregelt werden. Die Betreiber dürfen die Statistik Dritten nicht zur Kenntnis geben. Die Regulierungsbehörde überlässt den Ländern die Statistik unentgeltlich. Sie fasst die einzelnen Statistiken zusammen und nimmt das Ergebnis in ihren Bericht nach § 81 Abs. 1 auf.

§ 89
Datenschutz

(1) Die Bundesregierung erlässt für Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften zum Schutze personenbezogener Daten der an der Telekommunikation Beteiligten, welche die Erhebung, Verarbeitung und Nutzung dieser Daten regeln. Die Vorschriften haben dem Grundsatz der Verhältnismäßigkeit, insbesondere der Beschränkung der Erhebung, Verarbeitung und Nutzung auf das Erforderliche, sowie dem Grundsatz der Zweckbindung Rechnung zu tragen. Dabei sind Höchstfristen für die Speicherung festzulegen und insgesamt die berechtigten Interessen des jeweiligen Unternehmens und der Betroffenen zu berücksichtigen. Einzelangaben über juristische Personen, die dem Fernmeldegeheimnis unterliegen, stehen den personenbezogenen Daten gleich.

(2) Nach Maßgabe der Rechtsverordnung dürfen Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, die Daten natürlicher und juristischer Personen erheben, verarbeiten und nutzen, soweit dies erforderlich ist

1. zur betrieblichen Abwicklung ihrer jeweiligen geschäftsmäßigen Telekommunikationsdienste, nämlich für

   a) das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses,

   b) das Herstellen und Aufrechterhalten einer Telekommunikationsverbindung,

   c) das ordnungsgemäße Ermitteln und den Nachweis der Entgelte für geschäftsmäßige Telekommunikationsdienste einschließlich der auf andere Netzbetreiber und Anbieter von geschäftsmäßigen Telekommunikationsdiensten entfallenden Leistungsanteile; für den Nachweis ist dem Nutzer eine Wahlmöglichkeit hinsichtlich Speicherdauer und Speicherumfang einzuräumen,

   d) das Erkennen und Beseitigen von Störungen an Telekommunikationsanlagen,

   e) das Aufklären sowie das Unterbinden von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie der geschäftsmäßigen Telekommunikationsdienste, sofern tatsächliche Anhaltspunkte vorliegen; nach näherer Bestimmung in der Rechtsverordnung dürfen aus den Gesamtdatenbeständen die Daten ermittelt werden, die konkrete Indizien für eine missbräuchliche Inanspruchnahme von geschäftsmäßigen Telekommunikationsdiensten enthalten,

2. für das bedarfsgerechte Gestalten von geschäftsmäßigen Telekommunikationsdiensten; dabei dürfen Daten in bezug auf den Anschluss, von dem der Anruf ausgeht, nur mit Einwilligung des Anschlussinhabers verwendet und müssen Daten in bezug auf den angerufenen Anschluss unverzüglich anonymisiert werden,

3. auf schriftlichen Antrag eines Nutzers zum Zwecke

   a) der Darstellung der Leistungsmerkmale; hierzu dürfen insbesondere Datum, Uhrzeit, Dauer und Rufnummern der von seinem Anschluss hergestellten

Verbindungen unter Wahrung des in der Rechtsverordnung zu regelnden Schutzes von Mitbenutzern und Anrufen bei Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die gemäß ihrer von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannten Aufgabenbestimmung 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, mitgeteilt werden,

b) des Identifizierens von Anschlüssen, wenn er in einem zu dokumentierenden Verfahren schlüssig vorgetragen hat, das Ziel bedrohender oder belästigender Anrufe zu sein; dem Nutzer werden die Rufnummern der Anschlüsse sowie die von diesen ausgehenden Verbindungen und Verbindungsversuche einschließlich Name und Anschrift des Anschlussinhabers nur bekanntgegeben, wenn er zuvor die Anrufe nach Datum und Uhrzeit eingrenzt, soweit ein Missbrauch der Überwachungsmöglichkeit nicht auf andere Weise ausgeschlossen werden kann; grundsätzlich wird der Anschlussinhaber über die Auskunftserteilung nachträglich informiert.

(3) Es dürfen nur die näheren Umstände der Telekommunikation erhoben, verarbeitet und genutzt werden. Soweit es für Maßnahmen nach Absatz 2 Nr. 1 Buchstabe e unerlässlich ist, dürfen im Einzelfall Steuersignale maschinell erhoben, verarbeitet und genutzt werden; die Regulierungsbehörde ist hierüber in Kenntnis zu setzen. Der Betroffene ist zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahmen möglich ist. Die Erhebung, Verarbeitung und Nutzung anderer Nachrichteninhalte ist unzulässig, es sei denn, dass sie nach Absatz 4 notwendig oder im Einzelfall für Maßnahmen nach Absatz 5 unerlässlich ist.

(4) Beim geschäftsmäßigen Erbringen von Telekommunikationsdiensten dürfen Nachrichteninhalte nur aufgezeichnet, Dritten zugänglich gemacht oder sonst verarbeitet werden, soweit dies Gegenstand oder aus verarbeitungstechnischen Gründen Bestandteil des Dienstes ist. § 85 Abs. 3 Satz 3 bleibt unberührt.

(5) 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. Das Aufschalten muss den betroffenen Gesprächsteilnehmern durch ein akustisches Signal angezeigt und ausdrücklich mitgeteilt werden.

(6) Ferner haben die in Absatz 2 genannten Unternehmen und Personen personenbezogene Daten, die sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben, im Einzelfall auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist. Auskünfte an die genannten Stellen dürfen Kunden oder Dritten nicht mitgeteilt werden.

(7) Die in Absatz 2 genannten Unternehmen und Personen dürfen die personenbezogenen Daten, die sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben, verarbeiten und nutzen, soweit dies für Zwecke der Werbung, Kundenberatung oder Marktforschung für die in Absatz 2 genannten Unternehmen und Personen erforderlich ist und der Kunde eingewilligt hat. Personenbezogene Daten von Kunden, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes von den in Absatz 2 genannten Unternehmen und Personen bereits erhoben waren, dürfen für die in Satz 1 genannten Zwecke verarbeitet und genutzt werden, wenn der Kunde nicht widerspricht. Sein Einverständnis gilt als erteilt, wenn er in angemessener Weise über sein Widerspruchsrecht informiert worden ist und von seinem Widerspruchsrecht keinen Gebrauch gemacht hat.

(8) Diensteanbieter können Kunden mit ihrem Namen, ihrer Anschrift und zusätzlichen Angaben, wie Beruf, Branche, Art des Anschlusses und Mitbenutzer, in öffentliche gedruckte oder elektronische Verzeichnisse eintragen, soweit der Kunde dies beantragt hat. Dabei kann der Kunde bestimmen, welche Angaben in den Kundenverzeichnissen veröffentlicht werden sollen, dass die Eintragung nur in gedruckten oder elektronischen Verzeichnissen erfolgt oder dass jegliche Eintragung unterbleibt. Mitbenutzer dürfen eingetragen werden, soweit sie damit einverstanden sind. Sind Kunden beim Inkrafttreten dieses Gesetzes in ein Kundenverzeichnis eingetragen, so muss die Eintragung künftig unterbleiben, wenn der Kunde widerspricht. Absatz 7 Satz 3 gilt entsprechend.

(9) Nach Maßgabe der entsprechenden Rechtsverordnung dürfen Unternehmen und Personen im Sinne des Absatzes 2 im Einzelfall Auskunft über in öffentlichen Verzeichnissen enthaltene Daten der Nutzer von geschäftsmäßigen Telekommunikationsdiensten erteilen oder durch Dritte erteilen lassen. Die Auskunft darf nur über Daten von Kunden erteilt werden, die in angemessener Weise darüber

informiert worden sind, dass sie der Weitergabe ihrer Daten widersprechen können, und die von ihrem Widerspruchsrecht keinen Gebrauch gemacht haben. Ein Widerspruch ist in den Verzeichnissen des Diensteanbieters unverzüglich zu vermerken. Er ist auch von anderen Diensteanbietern zu beachten, sobald er in dem öffentlichen Verzeichnis des Diensteanbieters vermerkt ist.

(10) Die geschäftsmäßige Erbringung von Telekommunikationsdiensten und deren Entgeltfestlegung darf nicht von der Angabe personenbezogener Daten abhängig gemacht werden, die für die Erbringung oder Entgeltfestlegung dieser Dienste nicht erforderlich sind. Soweit die in Absatz 2 genannten Unternehmen die Verarbeitung oder Nutzung personenbezogener Daten eines Kunden von seiner Einwilligung abhängig machen, haben sie ihn in sachgerechter Weise über Inhalt und Reichweite der Einwilligung zu informieren. Dabei sind die vorgesehenen Zwecke und Nutzungszeiten zu nennen. Die Einwilligung muss ausdrücklich und in der Regel schriftlich erfolgen. Soll sie im elektronischen Verfahren erfolgen, ist dabei für einen angemessenen Zeitraum eine Rücknahmemöglichkeit vorzusehen.

§ 90
Auskunftsersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste anbietet, ist verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere vergeben werden, sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingenten aufzunehmen sind, auch soweit diese nicht in öffentliche Verzeichnisse eingetragen sind.

(2) Die aktuellen Kundendateien sind von dem Verpflichteten nach Absatz 1 verfügbar zu halten, so dass die Regulierungsbehörde einzelne Daten oder Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann. Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können.

(3) Auskünfte aus den Kundendateien nach Absatz 1 werden

1. den Gerichten, Staatsanwaltschaften und anderen Justizbehörden sowie sonstigen Strafverfolgungsbehörden,

2. den Polizeien des Bundes und der Länder für Zwecke der Gefahrenabwehr,

3. den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes und

4. den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst und dem Bundesnachrichtendienst

jederzeit unentgeltlich erteilt, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.

(4) Die Regulierungsbehörde hat die Daten, die in den Kundendateien der Verpflichteten nach Absatz 1 gespeichert sind, auf Ersuchen der in Absatz 3 genannten Stellen im automatisierten Verfahren abzurufen und an die ersuchende Stelle weiter zu übermitteln. Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlass besteht. Die Verantwortung für die Zulässigkeit der Übermittlung tragen die in Absatz 3 genannten Behörden. Die Regulierungsbehörde 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, die die Daten abrufende Person sowie die ersuchende Stelle und deren Aktenzeichen. Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig. Die Protokolldaten sind nach zwölf Monaten zu löschen.

(5) Absatz 1 gilt entsprechend für Dritte, die Rufnummern aus einem Rufnummernkontingent vergeben, ohne Verpflichteter im Sinne des Absatzes 1 zu sein, mit der Maßgabe, dass es dem Dritten überlassen bleibt, in welcher Form er die in Absatz 1 genannten Daten zur Auskunftserteilung vorhält. Er hat die Auskünfte aus den Kundendateien den in Absatz 3 genannten Behörden auf deren Ersuchen zu erteilen. Über die Tatsache einer Abfrage und die erteilten Auskünfte sowie über deren nähere Umstände hat der Auskunftspflichtige Stillschweigen, insbesondere gegenüber dem Betroffenen, zu wahren.

(6) Der Verpflichtete nach Absatz 1 hat alle Vorkehrungen in seinem Verantwortungsbereich auf seine Kosten zu treffen, die für den automatisierten Abruf gemäß Absatz 2 erforderlich sind. Dazu gehören auch, jeweils nach den Vorgaben der Regulierungsbehörde, 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.

(7) In den Fällen der Auskunftserteilung nach Absatz 5, in denen das Gesetz über die Entschädigung von Zeugen und Sachverständigen nicht gilt, sind die Vorschriften des genannten Gesetzes über die Höhe der Entschädigung entsprechend anzuwenden.

(8) Bei wiederholten Verstößen gegen die Absätze 1 und 2 kann die geschäftliche Tätigkeit des Verpflichteten durch Anordnung der Regulierungsbehörde dahingehend eingeschränkt werden, dass der Kundenstamm bis zur Erfüllung der sich aus diesen Vorschriften ergebenden Verpflichtungen außer durch Vertragsablauf oder Kündigung nicht verändert werden darf.

§ 91
Kontrolle und Durchsetzung von Verpflichtungen

(1) Die Regulierungsbehörde kann Anordnungen und andere geeignete Maßnahmen treffen, um die Einhaltung der Vorschriften des Elften Teils dieses Gesetzes und der auf Grund dieses Teils ergangenen Rechtsverordnungen sicherzustellen. Dazu können von den Verpflichteten erforderliche Auskünfte verlangt werden. Die Regulierungsbehörde ist zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- und Geschäftszeiten zu betreten und zu besichtigen.

(2) Zur Durchsetzung der Verpflichtungen, die Betreibern von Telekommunikationsanlagen durch eine Rechtsverordnung nach § 88 Abs. 2 auferlegt sind, kann die Regulierungsbehörde nach Maßgabe des Verwaltungsvollstreckungsgesetzes Zwangsgelder bis zu drei Millionen Deutsche Mark und zur Durchsetzung der Verpflichtungen nach § 90 Abs. 1 und 2 Zwangsgelder bis zu zweihunderttausend Deutsche Mark festsetzen.

(3) Bei Nichterfüllung von Verpflichtungen des Elften Teils dieses Gesetzes kann die Regulierungsbehörde 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 das Bundesministerium für Post und Telekommunikation und übermittelt diesem nach pflichtgemäßem Ermessen weitere Ergebnisse seiner Kontrolle.

(5) Das Fernmeldegeheimnis des Artikels 10 Grundgesetz wird eingeschränkt.

§ 92
Auskunftspflicht

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt, ist verpflichtet, dem Bundesministerium für Post und Telekommunikation 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 Artikel 1 § 3 des Gesetzes zu Artikel 10 Grundgesetz erforderlich ist. Die Verwendung einer nach dieser Vorschrift erlangten Auskunft zu anderen Zwecken ist auszuschließen. Das Bundesministerium für Post und Telekommunikation kann die Befugnis zu Anfragen nach Absatz 1 auf die Regulierungsbehörde übertragen.

§ 93
Staatstelekommunikationsverbindungen

Telekommunikationsunternehmen, die einen handvermittelten Telekommunikationsdienst anbieten, sind verpflichtet, gemäß den Regelungen der Konstitution der Internationalen Fernmeldeunion den Staatstelekommunikationsverbindungen im Rahmen des Möglichen Vorrang vor dem

übrigen Telekommunikationsverkehr einzuräumen, wenn dies von dem Anmelder der Verbindung ausdrücklich verlangt wird.

§ 94

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 65 Abs. 1 dort genannte Sendeanlagen

1. besitzt oder

2. herstellt, vertreibt, einführt oder sonst in den Geltungsbereich dieses Gesetzes verbringt.

(2) Handelt der Täter in den Fällen des Absatzes 1 Nr. 2 fahrlässig, so ist die Strafe Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.

§ 95

Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 86 Satz 1 oder 2 eine Nachricht abhört oder den Inhalt einer Nachricht oder die Tatsache ihres Empfangs einem anderen mitteilt.

§ 96
Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4 Satz 1 eine Anzeige nicht, nicht richtig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig erstattet,

2. entgegen § 5 einen Bericht nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zur Verfügung stellt,

3. ohne Lizenz nach § 6 Abs. 1 Übertragungswege betreibt oder Sprachtelefondienst anbietet,

4. entgegen § 14 Abs. 1 oder 2 Satz 1 Telekommunikationsdienstleistungen für die Öffentlichkeit nicht in rechtlich selbständigen Unternehmen führt oder die Nachvollziehbarkeit der finanziellen Beziehungen nicht oder nicht in der vorgeschriebenen Weise gewährleistet,

5. entgegen § 22 Abs. 1 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

6. ohne Genehmigung nach § 25 Abs. 1 ein Entgelt erhebt,

7. einer vollziehbaren Anordnung nach § 29 Abs. 2 Satz 2, auch in Verbindung mit § 30 Abs. 5 Satz 2, nach § 31 Abs. 1 Nr. 1, § 33 Abs. 2 Satz 1, auch in Verbindung mit § 38 Abs. 2, nach § 34 Abs. 1, § 43 Abs. 4 Satz 4, Abs. 5 Satz 1 oder Abs. 6 Satz 1, § 44 Abs. 2 oder § 49 Satz 2 zuwiderhandelt,

8. einer vollziehbaren Auflage nach § 32 zuwiderhandelt,

9. einer Rechtsverordnung nach § 35 Abs. 5 Satz 1, § 47 Abs. 4, § 59 Abs. 4 Satz 1, § 62 Abs. 1 Satz 1, § 63 Abs. 1 Satz 3, § 87 Abs. 3 Satz 1 oder § 89 Abs. 1 Satz 1 oder einer vollziehbaren Anordnung auf Grund einer solchen Rechtsverordnung zuwiderhandelt, soweit die Rechtsverordnung für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist,

10. ohne Frequenzzuteilung nach § 47 Abs. 1 Satz 1 Frequenzen nutzt,

11. entgegen § 60 Abs. 6 Satz 1 eine Ausfertigung der Erklärung über den Verwendungszweck nicht oder nicht rechtzeitig übermittelt,

12. entgegen § 65 Abs. 3 für eine Sendeanlage wirbt,

13. entgegen § 88 Abs. 2 Satz 4 Nr. 1 in Verbindung mit einer Rechtsverordnung nach § 88 Abs. 2 Satz 2 Nr. 1 den Betrieb einer Telekommunikationsanlage aufnimmt,

14. entgegen § 88 Abs. 2 Satz 4 Nr. 2 oder 3 den Betrieb einer Telekommunikationsanlage aufnimmt,

14a. entgegen § 88 Abs. 2 Satz 6 eine Einrichtung nicht oder nicht rechtzeitig nachbessert,

15. entgegen § 88 Abs. 4 Satz 1 einen Netzzugang nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bereitstellt oder

16. entgegen § 90 Abs. 2, Satz 1 eine Kundendatei nicht oder nicht in der vorgeschriebenen Weise verfügbar hält, entgegen § 90 Abs. 5 Satz 2 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt, entgegen § 90 Abs. 2 Satz 2 Kenntnis von Abrufen nimmt oder entgegen § 90 Abs. 5 Satz 3 Stillschweigen nicht wahrt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 3, 4, 6, 7, 8, 9, 10, 13 und 14a mit einer Geldbuße bis zu einer Million Deutsche Mark, in den Fällen des Absatzes 1 Nr. 1, 2, 5, 11, 12, 14, 15 und 16 mit einer Geldbuße bis zu zwanzigtausend Deutsche Mark geahndet werden. Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Regulierungsbehörde.

II.2 Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation vom 22.01.2002 (Telekommunikations-Überwachungsverordnung - TKÜV)

Teil 1
Allgemeine Vorschriften, Begriffsbestimmungen, Grundsätze

§ 1
Zweck der Verordnung

Zweck dieser Verordnung ist es,

1. die Anforderungen an die Gestaltung der technischen Einrichtungen zu regeln, die für die Umsetzung der

   a) in den §§ 100a und 100b der Strafprozessordnung,

   b) im Artikel 10-Gesetz mit Ausnahme von dessen §§ 5 und 8 sowie

   c) in den §§ 39 bis 43 des Außenwirtschaftsgesetzes

   vorgesehenen Maßnahmen zur Überwachung der Telekommunikation erforderlich sind, sowie organisatorische Grundsätze für die Umsetzung derartiger Maßnahmen mittels dieser Einrichtungen festzulegen,

2. das Genehmigungsverfahren und das Verfahren der Abnahme nach § 88 Abs. 2 Satz 2 Nr. 2 des Telekommunikationsgesetzes festzulegen,

3. gemäß § 88 Abs. 2 Satz 2 Nr. 3 des Telekommunikationsgesetzes zu bestimmen, bei welchen Telekommunikationsanlagen die durch § 88 Abs. 1 des Telekommunikationsgesetzes geforderten technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen nicht zu gestalten und vorzuhalten sind,

4. Regelungen für die gemäß § 88 Abs. 2 Satz 3 des Telekommunikationsgesetzes vorgesehenen Ausnahmefälle zu treffen, in denen von der Erfüllung einzelner technischer Anforderungen abgesehen werden kann,

5. die Anforderungen an die Netzzugänge nach § 88 Abs. 4 des Telekommunikationsgesetzes festzulegen, an die die Aufzeichnungseinrichtungen der berechtigten Stellen angeschlossen werden, sowie

6. die Ausgestaltung der gemäß § 88 Abs. 5 des Telekommunikationsgesetzes zu erstellenden Jahresstatistik festzulegen.

§ 2
Kreis der Verpflichteten

(1) Diese Verordnung gilt für die Betreiber von Telekommunikationsanlagen, mittels derer Telekommunikationsdienstleistungen für die Öffentlichkeit (§ 3 Nr. 19 des Telekommunikationsgesetzes) angeboten werden. Werden mit einer Telekommunikationsanlage sowohl Telekommunikationsdienstleistungen für die Öffentlichkeit als auch andere Telekommunikationsdienstleistungen erbracht, gilt diese Verordnung nur für den Teil der Telekommunikationsanlage, der der Erbringung von Telekommunikationsdienstleistungen für die Öffentlichkeit dient.

(2) Betreiber, die nicht unter Absatz 1 fallen, sind von der Pflicht befreit, technische Einrichtungen zur Umsetzung der gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und vorbereitende organisatorische Vorkehrungen für die Umsetzung solcher Maßnahmen zu treffen. Dies gilt ebenso für Telekommunikationsanlagen nach Absatz 1, soweit

1. es sich um ein Verbindungsnetz gemäß § 3 Nr. 23 des Telekommunikationsgesetzes handelt,
2. sie Netzknoten sind, die der Zusammenschaltung mit dem Internet dienen,
3. sie aus Übertragungswegen gebildet werden, die nicht dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dienen,
4. sie 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, oder
5. an sie nicht mehr als 1000 Teilnehmer angeschlossen sind.

Die Vorschriften des § 100b Abs. 3 Satz 1 der Strafprozessordnung, des § 2 Abs. 1 Satz 3 des Artikel 10-Gesetzes und des § 39 Abs. 5 des Außenwirtschaftsgesetzes bleiben unberührt.

§ 3
Grenzen des Anwendungsbereichs

Telekommunikation, bei der die Telekommunikationsanlage im Rahmen der üblichen Betriebsverfahren erkennt, dass sich das von der zu überwachenden Person genutzte Endgerät im Ausland befindet, ist nicht zu erfassen, es sei denn, die zu überwachende Telekommunikation wird an einen im Inland gelegenen Anschluss um- oder weitergeleitet.

§ 4
Begriffsbestimmungen

Im Sinne dieser Verordnung ist

1. Anordnung
   die Anordnung zur Beschränkung des Fernmeldegeheimnisses nach § 10 des Artikel 10-Gesetzes, § 100b der Strafprozessordnung oder § 40 des Außenwirtschaftsgesetzes;
2. Anschluss
   die netzseitige technische Einrichtung eines Netzzugangs gemäß § 3 Nr. 9 des Telekommunikationsgesetzes, der durch einen Teilnehmer mittels geeigneter Endgeräte genutzt wird;
3. berechtigte Stelle
   eine nach § 1 Abs. 1 Nr. 1 des Artikel 10-Gesetzes, § 100b Abs. 3 Satz 1 der Strafprozessordnung oder § 39 Abs. 1 Satz 1 des Außenwirtschaftsgesetzes zur Überwachung und Aufzeichnung der Telekommunikation berechtigte Stelle;
4. Endgerät
   die Endeinrichtung nach § 3 Nr. 3 des Telekommunikationsgesetzes, mittels derer ein Teilnehmer einen Anschluss zur Abwicklung seiner Telekommunikation nutzt;
5. Funkzelle
   der Versorgungsbereich innerhalb eines Mobilfunknetzes, der eine bestimmte geographische Fläche abdeckt;
6. Kennung
   das in der Anordnung angegebene, auf eine Person bezogene technische Merkmal zur Bezeichnung der Telekommunikation, die überwacht werden soll;
7. Kennzeichnung
   a) ein von der berechtigten Stelle vorgegebenes Merkmal zur eindeutigen Bezeichnung der zu überwachenden Kennung oder
   b) in Fällen, in denen eine bestimmte zu überwachende Telekommunikation für die Übermittlung an die berechtigte Stelle in zwei oder mehr Teile aufgeteilt wird und diese Teile zeitlich versetzt oder auf voneinander getrennten Wegen übermittelt werden, die vom Verpflichteten zu vergebenden eindeutigen Zuordnungsmerkmale, aufgrund derer diese Teile einander zweifelsfrei zugeordnet werden können;
8. Pufferung
   die kurzzeitige Zwischenspeicherung von Informationen zur Vermeidung von Informationsverlusten während systembedingter Wartezeiten;
9. Rufzone
   ein Versorgungsbereich in einem Funkrufnetz;

10. Speichereinrichtung
    eine netzseitige Einrichtung zur vertragsgemäßen, teilnehmerorientierten Speicherung von Telekommunikation;

11. Teilnehmer
    eine Person, die das Angebot von Telekommunikation oder Telekommunikationsdienstleistungen für eigene Telekommunikationszwecke nutzt;

12. Übergabepunkt
    der Punkt der technischen Einrichtungen des Verpflichteten, an dem er die Kopie der zu überwachenden Telekommunikation für die Übermittlung an die berechtigte Stelle bereitstellt; der Übergabepunkt kann als systeminterner Übergabepunkt gestaltet sein, der am Ort der Telekommunikationsanlage nicht physikalisch dargestellt ist;

13. Überwachungsmaßnahme
    eine Maßnahme zur Überwachung der Telekommunikation nach § 3 des Artikel 10-Gesetzes, den §§ 100a, 100b der Strafprozessordnung oder den §§ 39 bis 43 des Außenwirtschaftsgesetzes;

14. Verpflichteter
    der Betreiber einer Telekommunikationsanlage gemäß § 2 Abs. 1, soweit sie nicht unter die Ausnahmeregelungen des § 2 Abs. 2 Satz 2 fällt;

15. zu überwachende Telekommunikation

    die Telekommunikation, die auf Grund der erlassenen Anordnung der Überwachung unterliegt; sie umfasst jede Telekommunikation, die

    a) von der zu überwachenden Rufnummer oder anderen Kennung ausgeht, auch soweit sie der auf Teilnehmereingaben beruhenden Steuerung von Betriebsmöglichkeiten der zu überwachenden Kennung dient,

    b) für die zu überwachende Rufnummer oder andere Kennung bestimmt ist,

    c) in eine Speichereinrichtung, die der zu überwachenden Rufnummer oder anderen Kennung zugeordnet ist, eingestellt oder aus dieser abgerufen wird oder

    d) zu einer der zu überwachenden Kennung aktuell zugeordneten anderen Zieladresse um- oder weitergeleitet wird,

    und besteht aus den Informationen, die zwischen den Telekommunikationspartnern oder den von ihnen genutzten Speichereinrichtungen übermittelt werden (Inhalt), und den Daten über die die jeweilige Telekommunikation bezeichnenden näheren Umstände.

§ 5
Grundsätze

(1) Zur Umsetzung einer Überwachungsmaßnahme hat der Verpflichtete der berechtigten Stelle am Übergabepunkt eine vollständige Kopie der Telekommunikation bereitzustellen, die über seine Telekommunikationsanlage unter der in der Anordnung angegebenen Kennung abgewickelt wird. Dabei hat er sicherzustellen, dass die bereitgestellten Daten keine nicht durch die Anordnung bezeichnete Telekommunikation enthalten.

(2) Der Verpflichtete hat sicherzustellen, dass er die Umsetzung einer Überwachungsmaßnahme eigenverantwortlich vornehmen kann. In diesem Rahmen ist die Wahrnehmung der im Überwachungsfall erforderlichen Tätigkeiten durch einen Erfüllungsgehilfen zulässig, der jedoch nicht der berechtigten Stellen angehören darf.

(3) Der Verpflichtete hat sicherzustellen, dass die technische Umsetzung einer Überwachungsmaßnahme weder von den an der Telekommunikation Beteiligten noch von Dritten feststellbar ist. Insbesondere dürfen die Betriebsmöglichkeiten des Anschlusses, der durch die zu überwachende Kennung genutzt wird, durch die technische Umsetzung einer Überwachungsmaßnahme nicht verändert werden.

(4) Der Verpflichtete hat der berechtigten Stelle unmittelbar nach Abschluss der für die technische Umsetzung einer Überwachungsmaßnahme erforderlichen Tätigkeiten den Zeitpunkt des tatsächlichen Einrichtens der Überwachungsmaßnahme sowie die durch diese Tätigkeiten tatsächlich betroffene Kennung mitzuteilen. Dies gilt sinngemäß für die Übermittlung einer entsprechenden Information zum Zeitpunkt der Beendigung einer Überwachungsmaßnahme.

(5) Der Verpflichtete hat Engpässe, die bei gleichzeitiger Durchführung mehrerer Überwachungsmaßnahmen auftreten, unverzüglich zu beseitigen.

Teil 2
Technische Anforderungen

§ 6
Grundlegende Anforderungen an die technischen Einrichtungen

(1) Der Verpflichtete hat die zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen so zu gestalten, dass er eine Anordnung unverzüglich umsetzen kann.

(2) Der Verpflichtete hat sicherzustellen, dass die Verfügbarkeit seiner für die Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen der Verfügbarkeit seiner Telekommunikationsanlage entspricht, soweit dies mit vertretbarem Aufwand realisierbar ist.

(3) Der Verpflichtete hat seine für die Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen so zu gestalten, dass er die Überwachung aufgrund jeder Kennung ermöglichen kann, die für die technische Abwicklung der Telekommunikation in seiner Telekommunikationsanlage benutzt wird.

(4) Der Verpflichtete muss sicherstellen, dass er die Überwachung derselben Kennung gleichzeitig für mehr als eine berechtigte Stelle ermöglichen kann.

§ 7
Bereitzustellende Daten

(1) Der Verpflichtete hat der berechtigten Stelle als Teil der durch die zu überwachende Kennung bezeichneten Telekommunikation auch die folgenden bei ihm vorhandenen Daten bereitzustellen:

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 Kennung, auch wenn keine Telekommunikation mit der Gegenstelle zustande kommt oder wenn die gewählte Rufnummer oder die andere Kennung bei vorzeitiger Beendigung eines im Telekommunikationsnetz begonnenen Telekommunikationsversuches unvollständig bleibt und
   b) sofern die zu überwachende Telekommunikation an ein anderes als das von der zu überwachenden Kennung gewählte Ziel um- oder weitergeleitet wird, auch die Rufnummer oder andere Kennung des Um- oder Weiterleitungsziels, bei mehrfach gestaffelten Um- oder Weiterleitungen die Rufnummern oder anderen Kennungen der einzelnen Um- oder Weiterleitungsziele;
3. in Fällen, in denen die zu überwachende Kennung Ziel der Telekommunikation ist, die Rufnummer oder andere Kennung, von der aus die zu überwachende Kennung angewählt wurde, auch wenn keine Telekommunikation mit der Gegenstelle zustande kommt oder 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 einem beliebigen Anschluss zugeordnet wird, die Rufnummer oder andere Kennung dieses Anschlusses;
5. in Fällen, in denen der Teilnehmer für eine bestimmte Telekommunikation ein von dem Verpflichteten angebotenes Dienstmerkmal in Anspruch nimmt, die Angabe dieses Dienstmerkmals einschließlich dessen Kenngrößen;

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;

7. bei einer zu überwachenden Kennung aus Mobilfunknetzen

   a) Angaben zum Standort des Mobilanschlusses oder

   b) falls die Standortangaben nach Buchstabe a nicht verfügbar sind, die Bezeichnungen der Funkzellen oder der Rufzonen, über die der Mobilanschluss versorgt wird, sowie Angaben zu deren geographischer Lage;

   zur Umsetzung von Anordnungen, auf Grund derer Angaben zum Standort von mobilen Endgeräten verlangt werden, die empfangsbereit sind, kann der Verpflichtete seine technischen Einrichtungen so gestalten, dass sie diese Angaben in dem in der Telekommunikationsanlage üblichen Format und Umfang 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) Beginn der Telekommunikation oder des Telekommunikationsversuchs mit Datum und Uhrzeit,

      bb) Ende der Telekommunikation mit Datum und Uhrzeit,

      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.

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 anderen Daten kann verzichtet werden, solange diese Daten unverändert bleiben.

(2) Der Verpflichtete hat jede bereitgestellte Kopie der zu überwachenden Telekommunikation und die Daten nach Absatz 1 Satz 1 durch die von der berechtigten Stelle vorgegebene Kennzeichnung der jeweiligen Überwachungsmaßnahme zu bezeichnen, sofern der berechtigten Stelle diese Kopie unter Nutzung von Telekommunikationsnetzen mit Vermittlungsfunktionen übermittelt wird. In Fällen, in

denen die Kopie der zu überwachenden Telekommunikation und die Daten nach Absatz 1 Satz 1 für die Übermittlung an die berechtigte Stelle in zwei oder mehr Teile aufgeteilt wird und diese Teile zeitlich versetzt oder auf voneinander getrennten Wegen übermittelt werden, hat der Verpflichtete alle Teile zusätzlich dergestalt zu kennzeichnen, dass sie einander zweifelsfrei zugeordnet werden können.

(3) In Fällen, in denen die technischen Einrichtungen des Verpflichteten so gestaltet sind, dass die Daten nach Absatz 1 Satz 1 und die Kennzeichnung nach Absatz 2 Satz 1 getrennt von der Kopie der zu überwachenden Telekommunikation bereitgestellt werden, muss es möglich sein, der berechtigten Stelle ausschließlich diese Datensätze zu übermitteln, sofern dies im Einzelfall in der Anordnung ausdrücklich bestimmt wird.

(4) Die Absätze 1 bis 3 gelten entsprechend 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 zugrunde liegenden Technologie. Die tatsächliche technische Darstellung der geforderten Angaben hat der Verpflichtete in Abhängigkeit von der seiner Telekommunikationsanlage zugrunde liegenden Technologie zu gestalten.

§ 8
Übergabepunkt

(1) Der Verpflichtete hat die zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen so zu gestalten, dass die Kopie der zu überwachenden Telekommunikation an dem gemäß § 18 genehmigten Übergabepunkt bereitgestellt wird.

(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 durch die zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen des Verpflichteten erfolgen kann;
2. an ihm ausschließlich die Kopie der durch die Anordnung bezeichneten zu überwachenden Telekommunikation bereitgestellt wird;

3. der berechtigten Stelle die Kopie der zu überwachenden Telekommunikation grundsätzlich in dem Format bereitgestellt wird, in dem dem Verpflichteten die zu überwachende Telekommunikation vorliegt;
4. die Qualität der an dem Übergabepunkt bereitgestellten Kopie grundsätzlich nicht schlechter ist als die der zu überwachenden Telekommunikation;
5. der berechtigten Stelle die Anteile der Telekommunikation, welche das der zu überwachenden Kennung zugeordnete Endgerät empfängt, und die Anteile der Telekommunikation, die dieses Endgerät sendet, grundsätzlich getrennt bereitgestellt werden; 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 Kopie der zu überwachenden Telekommunikation an die berechtigte Stelle benutzt wird, Bestandteile des Übergabepunktes sind und
7. hinsichtlich der Fähigkeit zur Übermittlung der Kopie der zu überwachenden Telekommunikation an die jeweils berechtigte Stelle folgende Anforderungen erfüllt werden:
   a) die Übermittlung der bereitgestellten Kopie der zu überwachenden Telekommunikation an die berechtigte Stelle erfolgt grundsätzlich unter Nutzung geeigneter Telekommunikationsnetze mit Vermittlungsfunktionen oder genormter, allgemein verfügbarer Übertragungswege und Übertragungsprotokolle,
   b) die Übermittlung der Kopie der zu überwachenden Telekommunikation vom Übergabepunkt zu den entsprechenden Anschlüssen bei den berechtigten Stellen wird ausschließlich von den technischen Einrichtungen des Verpflichteten jeweils unmittelbar nach dem Erkennen einer zu überwachenden Telekommunikation eingeleitet und
   c) die Schutzanforderungen gemäß § 14 Abs. 2 werden unterstützt.

Muss in begründeten Ausnahmefällen bei bestimmten Telekommunikationsanlagen von dem Grundsatz nach Satz 1 Nr. 3 abgewichen werden, hat der Verpflichtete dies in den Antragsunterlagen nach § 18 Abs. 2 und 3 so darzulegen, dass die technischen Einzelheiten nachvollziehbar sind. Auf die Richtungstrennung nach Satz 1 Nr. 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 die unbefugte Kenntnisnahme durch Dritte schützt, hat er die von ihm für diese Telekommunikation angewendeten Schutzvorkehrungen bei der an dem Übergabepunkt bereitzustellenden Kopie der zu überwachenden Telekommunikation aufzuheben oder der berechtigten Stelle technische

Einrichtungen oder Verfahren bereitzustellen, die ihr die nach Möglichkeit zeitgleiche Kenntnisnahme der ungeschützten Telekommunikation ermöglichen. § 14 Abs. 2 bleibt unberührt.

§ 9
Übermittlung der Kopie der zu überwachenden Telekommunikation

(1) Die Übermittlung der Kopie der zu überwachenden Telekommunikation einschließlich der Daten nach § 7 Abs. 1 Satz 1 und der Kennzeichnungen nach § 7 Abs. 2 vom Übergabepunkt an die berechtigte Stelle soll über Telekommunikationsnetze mit Vermittlungsfunktionen erfolgen. Dem Verpflichteten werden hierzu von der berechtigten Stelle für jede zu überwachende Kennung die Anschlüsse benannt, an die die Kopie der zu überwachenden Telekommunikation zu übermitteln ist und die so gestaltet sind, dass die Kopien mehrerer gleichzeitig stattfindender zu überwachender Telekommunikationen entgegengenommen werden können. Die Kennungen der Anschlüsse der berechtigten Stelle können voneinander abweichen, wenn die Kopie der zu überwachenden Telekommunikation und die zugehörigen Daten nach § 7 Abs. 1 Satz 1 einschließlich der Kennzeichnungen nach § 7 Abs. 2 über voneinander getrennte Wege oder über Netze mit unterschiedlicher Technologie übermittelt werden. Für die Entgegennahme der Kopie solcher Telekommunikation, die der Verpflichtete im Rahmen der von ihm angebotenen Dienstleistung in einer der zu überwachenden Kennung zugeordneten Speichereinrichtung speichert, kann die berechtigte Stelle gesonderte Anschlüsse benennen, auch getrennt nach unterschiedlichen Diensten, sofern der Verpflichtete die gespeicherte Telekommunikation nach Diensten unterscheidet. Wird die Kopie der zu überwachenden Telekommunikation über Telekommunikationsnetze mit Vermittlungsfunktionen übermittelt, ist deren Inanspruchnahme auf die für die Übermittlung erforderliche Zeitdauer zu begrenzen.

(2) Ist zum Zeitpunkt der Gestaltung der technischen Einrichtungen ersichtlich, dass für die Übermittlung der Kopie der zu überwachenden Telekommunikation an die berechtigte Stelle kein geeignetes Telekommunikationsnetz mit Vermittlungsfunktionen zur Verfügung steht, hat der Verpflichtete in den vorzulegenden Antragsunterlagen eine andere geeignete Übermittlungsmöglichkeit vorzusehen, über deren Zulässigkeit die Regulierungsbehörde für Telekommunikation und Post im Rahmen des Genehmigungsverfahrens entscheidet.

(3) Maßnahmen zum Schutz der zu übermittelnden Kopie richten sich nach § 14.

§ 10
Zeitweilige Übermittlungshindernisse

Der Verpflichtete hat die zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen so zu gestalten, dass die Daten nach § 7 Abs. 1 Satz 1 und die Kennzeichnungen nach § 7 Abs. 2 in Fällen, in denen die Übermittlung der Kopie der zu überwachenden Telekommunikation an die berechtigte Stelle ausnahmsweise nicht möglich ist, unverzüglich nachträglich übermittelt werden. Eine Verhinderung oder Verzögerung der zu überwachenden Telekommunikation oder eine Speicherung der Kopie der zu überwachenden Telekommunikation aus diesen Gründen ist nicht zulässig. Eine für den ungestörten Funktionsablauf aus technischen, insbesondere übermittlungstechnischen Gründen erforderliche Pufferung der Kopie bleibt von Satz 2 unberührt.

§ 11
Technische Richtlinie

Die Regulierungsbehörde für Telekommunikation und Post erarbeitet unter Beteiligung der Verpflichteten, der Hersteller der technischen Einrichtungen, der berechtigten Stellen sowie der Hersteller der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen einen Vorschlag für eine Technische Richtlinie, in der die technischen Einzelheiten zu § 5 Abs. 4 und 5, § 6 Abs. 3, § 7 Abs. 1, 2 und 4, § 8 Abs. 2, § 9 Abs. 1, § 10 Satz 1 und 3, § 14 Abs. 1 und 2 Satz 1 bis 4 sowie die erforderlichen technischen Eigenschaften der Anschlüsse nach § 24 Abs. 1 Satz 2 in Abhängigkeit von den den Telekommunikationsanlagen zugrunde liegenden Technologien festzulegen sind. Dabei sind vorhandene Standards so weit wie möglich zu berücksichtigen. In gleicher Weise ist die Technische Richtlinie an den jeweiligen Stand der Technik anzupassen. Das Bundesministerium für Wirtschaft und Technologie erlässt die Technische Richtlinie im Benehmen mit dem Bundeskanzleramt, dem Bundesministerium des Innern, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen und dem Bundesministerium der Verteidigung als bei der Genehmigung nach § 88 des Telekommunikationsgesetzes zu berücksichtigende Verwaltungsvorschrift für die Regulierungsbehörde für Telekommunikation und Post. Die Technische Richtlinie und ihre Änderungen sind in geeigneter Weise bekannt zu geben.

Teil 3
Organisatorische Anforderungen, Schutzanforderungen

§ 12
Entgegennahme der Anordnung

(1) Der Verpflichtete hat sicherzustellen, dass er jederzeit über das Vorliegen einer Anordnung und die Dringlichkeit ihrer Umsetzung benachrichtigt werden kann. Darüber hinaus hat er 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 innerhalb von 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 eine im Inland belegene Stelle anzugeben, für deren Erreichbarkeit er den berechtigten Stellen keine Anschlüsse benennen darf, bei denen dem Anrufer Entgelte berechnet werden, die über die Entgelte für eine einfache Telekommunikationsverbindung hinausgehen.

(2) In Fällen, in denen die berechtigte Stelle eine besondere Dringlichkeit geltend macht, hat der Verpflichtete die zur Umsetzung einer Überwachungsmaßnahme erforderlichen Schritte aufgrund einer ihm vorab per Telefax oder auf gesichertem elektronischen Weg übermittelten Kopie der Anordnung einzuleiten, nachdem er sich durch unverzüglichen Rückruf bei einer vorher vereinbarten Stelle davon überzeugt hat, dass die Kopie von einer berechtigten Stelle abgesandt wurde. Eine auf einer derartigen Grundlage eingeleitete Überwachungsmaßnahme hat der Verpflichtete wieder abzuschalten, sofern ihm das Original oder eine beglaubigte Abschrift der Anordnung nicht binnen drei Tagen nach Übermittlung der Kopie vorgelegt wird.

§ 13
Entstörung, Störungsmeldungen

Der Verpflichtete hat die unverzügliche Entstörung seiner für die Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen sicherzustellen. Während einer Überwachungsmaßnahme hat der Verpflichtete die betroffenen berechtigten Stellen unverzüglich über Störungen seiner zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen zu verständigen. Dabei sind anzugeben

1. die Art der Störung und deren Auswirkungen auf die laufenden Überwachungsmaßnahmen sowie
2. der Beginn und die voraussichtliche Dauer der Störung.

Nach Behebung der Störung sind die betroffenen berechtigten Stellen unverzüglich über den Zeitpunkt zu verständigen, ab dem die technischen Einrichtungen wieder ordnungsgemäß zur Verfügung stehen. In Mobilfunknetzen sind die Angaben gemäß den Sätzen 2 bis 4 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 gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, 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.

(2) Die Kopie der zu überwachenden Telekommunikation und deren Übermittlung an die berechtigte Stelle sind angemessen zu schützen gegen

1. Übermittlung an nichtberechtigte Anschlüsse,

2. unbefugte Belegung der Anschlüsse der berechtigten Stelle und

3. unbefugte Kenntnisnahme durch Dritte.

Grundsätzlich ist bei jeder Übermittlung der Kopie der zu überwachenden Telekommunikation über Telekommunikationsnetze mit Vermittlungsfunktionen die Empfangsberechtigung des Anschlusses der berechtigten Stelle und die Sendeberechtigung des Übergabepunktes des Verpflichteten durch technische Maßnahmen festzustellen. In Fällen, in denen die Verwaltung und Bestätigung von Nutzungsrechten für den Kreis der Verpflichteten oder der berechtigten Stellen erforderlich wird, sind die Aufgaben nach Satz 2 von einer Stelle außerhalb der zur Überwachung der Telekommunikation berechtigten Stellen wahrzunehmen. Sollen die Schutzziele nach Satz 1 Nr. 1 und 2 im Rahmen einer Geschlossenen Benutzergruppe erreicht werden, darf hierfür ausschließlich eine eigens für diesen Zweck eingerichtete Geschlossene Benutzergruppe genutzt werden, die durch die Regulierungsbehörde für Telekommunikation und Post verwaltet wird. Die Schutzanforderung nach Satz 1 Nr. 3 gilt bei der Übermittlung der Kopie der zu überwachenden Telekommunikation an die berechtigte Stelle über festgeschaltete Übertragungswege oder über Telekommunikationsnetze mit leitungsvermittelnder Technik aufgrund der diesen Übertragungsmedien zugrunde 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 zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen und auf Seite der berechtigten Stelle Bestandteil der Aufzeichnungs- und Auswertungseinrichtungen.

(3) Im Übrigen erfolgt die Umsetzung von Überwachungsmaßnahmen 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.

§ 15
Verschwiegenheit

(1) Der Verpflichtete darf Informationen über die Art und Weise, wie Überwachungsmaßnahmen in seiner Telekommunikationsanlage durchgeführt werden, Unbefugten nicht zugänglich machen.

(2) Der Verpflichtete hat den Schutz der im Zusammenhang mit Überwachungsmaßnahmen stehenden Informationen sicherzustellen. Dies gilt insbesondere für Informationen darüber, welche und wie viele Kennungen einer Überwachung unterliegen oder unterlegen haben und in welchen Zeiträumen Überwachungsmaßnahmen durchgeführt worden sind.

§ 16
Protokollierung

(1) Der Verpflichtete hat sicherzustellen, dass jede Nutzung der für die Umsetzung von Überwachungsmaßnahmen vorgesehenen technischen Einrichtungen und Funktionen, 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 Nutzungen für unternehmensinterne Testzwecke, für Zwecke der Abnahmemessungen (§ 19 Abs. 2), für Messungen bei Änderungen der Telekommunikationsanlage oder bei nachträglich festgestellten Mängeln (§ 20) und für die Mitwirkung bei Funktionsprüfungen der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen (§ 23) sowie solche Nutzungen, die durch fehlerhafte oder missbräuchliche Eingabe, Bedienung oder Schaltung verursacht wurden. Es sind zu protokollieren:

1. die Kennzeichnung nach § 7 Abs. 2 Satz 1 oder eine unternehmensinterne Bezeichnung der Überwachungsmaßnahme,
2. die tatsächlich eingegebene Kennung, auf Grund derer die für die Umsetzung von Überwachungsmaßnahmen vorgesehenen technischen Einrichtungen die zu überwachende Telekommunikation bereitstellen,
3. die Zeitpunkte (Datum und Uhrzeit auf der Grundlage der amtlichen Zeit), zwischen denen die für die Umsetzung von Überwachungsmaßnahmen vorgesehenen

technischen Einrichtungen die Telekommunikation in Bezug auf die Kennung nach Nummer 2 erfassen,

4. die Rufnummer oder die andere Kennung des Anschlusses, an das die Kopie der Telekommunikation weitergeleitet wird,
5. ein Merkmal zur Erkennung der jeweiligen Person, die diese Eingaben macht,
6. Datum und Uhrzeit der Eingabe.

Die Angaben nach Satz 3 Nr. 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 Zugriffs- und Löschfunktionen folgende Anforderungen eingehalten werden:

1. das Personal, das mit der praktischen Umsetzung von Überwachungsmaßnahmen 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 der Protokolle verantwortlichen Personal des Verpflichteten verfügbar sein;
3. die Nutzung der Löschfunktionen nach Nummer 2 ist unter Angabe des Zeitpunktes und eines Merkmals zur Erkennung der die Funktion jeweils nutzenden Person in einer Datei zu protokollieren, deren Daten frühestens nach zwei Jahren überschrieben werden dürfen;
4. die Berechtigungen zum Zugriff auf die Funktionen von Datenverarbeitungsanlagen oder auf die Datenbestände, die für die Prüfung der Protokolle oder die Erteilung von Zugriffsrechten erforderlich sind, dürfen nicht ohne Nachweis eingerichtet, geändert oder gelöscht werden können; dies kann durch die Dokumentation aller vergebenen, geänderten und zurückgezogenen Zugriffsberechtigungen in einer nicht löschbaren Datei erfolgen, deren Daten frühestens zwei Jahre nach deren Erhebung überschrieben werden dürfen.

§ 17
Prüfung der Protokolle

(1) Der Verpflichtete hat die protokollierten Datensätze auf Übereinstimmung mit den vorgelegten Anordnungen zu prüfen; dies soll zu Beginn eines jeden Kalendervierteljahres erfolgen. In den geheimschutzbetreuten Unternehmen obliegt diese Aufgabe dem Sicherheitsbevollmächtigten. Das mit der Prüfung betraute Personal kann zur Klärung von Zweifelsfällen das mit der praktischen Umsetzung der Überwachungsmaßnahmen betraute Personal hinzuziehen. Die unternehmensinterne Festlegung kürzerer Prüfzeiträume ist zulässig. Der Verpflichtete hat die Ergebnisse der Prüfungen schriftlich festzuhalten. Sind keine Beanstandungen aufgetreten, darf in den

Prüfergebnissen die nach § 16 Abs. 1 Satz 3 Nr. 2 protokollierte Kennung nicht mehr vermerkt sein und kann auf die übrigen Angaben gemäß § 16 Abs. 1 Satz 3 verzichtet werden. Der Verpflichtete hat eine Kopie der Prüfergebnisse an die Regulierungsbehörde für Telekommunikation und Post zu übersenden, die sie bis zum Ende des folgenden Kalenderjahres aufbewahrt.

(2) Bei Beanstandungen, insbesondere auf Grund unzulässiger Eingaben oder unzureichender Angaben, hat der Verpflichtete unverzüglich eine Untersuchung der Angelegenheit einzuleiten und die Regulierungsbehörde für Telekommunikation und Post 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 außerhalb einer Protokollprüfung Kenntnis über einen zu beanstandenden Sachverhalt erhält. Das Ergebnis der Untersuchung ist schriftlich festzuhalten. Der Verpflichtete hat eine Kopie der Untersuchungsergebnisse an die Regulierungsbehörde für Telekommunikation und Post zu übersenden, die sie bis zum Ende des folgenden Kalenderjahres aufbewahrt.

(3) Sofern kein Grund für eine Beanstandung vorliegt und die Überwachungsmaßnahme während des Zeitraumes, auf den sich die Prüfung bezieht, beendet worden ist, hat der Verpflichtete nach Ablauf des auf die Prüfung folgenden Kalendervierteljahres die nicht zu beanstandenden Datensätze zu löschen und die entsprechenden Anordnungen und alle zugehörigen Unterlagen einschließlich der für die jeweilige Überwachungsmaßnahme angefertigten unternehmensinternen Hilfsmittel zu vernichten. Ist die Überwachungsmaßnahme im Prüfzeitraum nicht beendet worden, sind die entsprechenden Datensätze, Anordnungen und alle zugehörigen Unterlagen einschließlich der für die jeweilige Überwachungsmaßnahme angefertigten unternehmensinternen Hilfsmittel weiterhin aufzubewahren.

(4) Für die Löschung der beanstandeten Protokolldaten und die Vernichtung der zugehörigen Unterlagen nach Abschluss der gemäß Absatz 2 durchzuführenden Untersuchungen gilt Absatz 3 Satz 1 vorbehaltlich anderer Rechtsvorschriften sinngemäß mit der Maßgabe, dass an die Stelle des dort genannten Zeitpunktes für die Löschung der Datensätze und die Vernichtung der Unterlagen der Ablauf des Kalendervierteljahres tritt, das auf den Abschluss der Untersuchung folgt.

(5) Andere Rechtsvorschriften, die eine längere Aufbewahrungszeit für Unterlagen vorschreiben, bleiben unberührt. Dies gilt auch für unternehmensinterne Vorgaben zur Aufbewahrung von Abrechnungsunterlagen.

(6) Die Regulierungsbehörde für Telekommunikation und Post ist befugt, Einsicht in die Protokolle, Anordnungen und die zugehörigen Unterlagen zu nehmen. Die Befugnisse der zuständigen Datenschutzbehörden werden durch die Absätze 1 bis 5 nicht berührt. Für die gemäß § 16 erstellten Protokolle muss für die Kontrollen nach den Sätzen 1 und 2

die Möglichkeit bestehen, die protokollierten Datensätze sowohl nach ihrer Entstehungszeit als auch nach den betroffenen Kennungen sortiert auszugeben.

Teil 4
Genehmigungsverfahren, Abnahme

§ 18
Genehmigungsverfahren

(1) Die Genehmigung nach § 88 Abs. 2 Satz 1 des Telekommunikationsgesetzes wird bei Vorliegen der Genehmigungsvoraussetzungen als Einzelgenehmigung erteilt.

(2) Der Verpflichtete hat vor der Inbetriebnahme der Telekommunikationsanlage oder vor der Einführung eines Telekommunikationsdienstes, der Auswirkungen auf Überwachungsmöglichkeiten hat, bei der Regulierungsbehörde für Telekommunikation und Post einen schriftlichen Antrag auf Genehmigung der technischen Gestaltung der von ihm zur Umsetzung von Überwachungsmaßnahmen vorgesehenen technischen Einrichtungen zu stellen. Für bauartgleiche Einrichtungen ist ein Antrag ausreichend. In dem Antrag sind Angaben zu machen über Namen und Sitz des Antragstellers sowie der Personen, die für den Antrag und für die Gestaltung der zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen verantwortlich sind. Die Regulierungsbehörde für Telekommunikation und Post kann zur Vereinheitlichung der Form der einzureichenden Unterlagen einen Musterantrag erstellen, auf dessen Verfügbarkeit im Amtsblatt der Regulierungsbehörde für Telekommunikation und Post hinzuweisen ist.

(3) Dem Antrag gemäß Absatz 2 sind die zur Prüfung der Genehmigungsvoraussetzungen erforderlichen Unterlagen über die Telekommunikationsanlage beizufügen. Die Unterlagen müssen insbesondere Beschreibungen enthalten über:

1. die technische Gestaltung der Telekommunikationsanlage einschließlich der geplanten Telekommunikationsdienste und der zugehörigen Dienstmerkmale,
2. die für die technische Umsetzung von Überwachungsmaßnahmen in Bezug auf diese Telekommunikationsanlage oder auf die jeweiligen Telekommunikationsdienste auswertbaren Kennungen,
3. die technischen Einrichtungen, die der Bereitstellung der Kopie der zu überwachenden Telekommunikation einschließlich der Daten gemäß § 7 Abs. 1 bis 4 sowie § 10 dienen,
4. den Übergabepunkt gemäß § 8 und die Bereitstellung der Kopie der zu überwachenden Telekommunikation gemäß § 9 sowie

5. die technischen Einrichtungen und die organisatorischen Vorkehrungen zur Umsetzung der Vorschriften gemäß der §§ 5, 6, 12 und 13 Satz 1, des § 14 Abs. 1, 2 Satz 1 bis 4 und Abs. 3 sowie der §§ 16 und 17 Abs. 1 Satz 1 und 2.

Zur Vereinfachung des Genehmigungsverfahrens kann der Verpflichtete bei den einzureichenden Antragsunterlagen auf ein von der Regulierungsbehörde für Telekommunikation und Post geprüftes Rahmenkonzept des Herstellers der Telekommunikationsanlage zurückgreifen, dem das Bundesministerium für Wirtschaft und Technologie zugestimmt hat. Soweit Unterlagen Geschäfts- oder Betriebsgeheimnisse enthalten, sind die Unterlagen entsprechend zu kennzeichnen. Im Falle der Fortschreibung der Unterlagen, insbesondere im Zusammenhang mit Abweichungen wie nach § 19 Abs. 3 Satz 3 und Änderungen wie nach § 20, sind der Regulierungsbehörde für Telekommunikation und Post Ausfertigungen der geänderten Seiten der Antragsunterlagen zusammen mit einer Liste der jeweils insgesamt gültigen Dokumente vorzulegen.

(4) Die Regulierungsbehörde für Telekommunikation und Post bestätigt dem Antragsteller den Eingang des Antrags. Sie prüft den Antrag und die mit ihm vorgelegten Unterlagen darauf, ob die vorgesehene Gestaltung der zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen den Anforderungen gemäß Satz 3 entspricht. Entsprechen die vorgelegten Unterlagen den Vorschriften der §§ 5, 6 und 7 Abs. 1 bis 4, der §§ 8 bis 10, 12 und 13 Satz 1, des § 14 Abs. 1, 2 Satz 1 bis 4 und Abs. 3, der §§ 16 und 17 Abs. 1 Satz 1 und 2 sowie den Anforderungen der Technischen Richtlinie nach § 11, wobei die Zulässigkeit von Abweichungen gemäß § 21 oder § 22 und die Übergangsfristen gemäß § 26 zu berücksichtigen sind, erteilt die Regulierungsbehörde für Telekommunikation und Post die Genehmigung gemäß § 88 Abs. 2 Satz 1 des Telekommunikationsgesetzes. Dabei ist darauf hinzuweisen, dass die tatsächliche Gestaltung der zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen entsprechend den Genehmigungsvoraussetzungen der Regulierungsbehörde für Telekommunikation und Post im Rahmen einer Abnahme nach § 88 Abs. 2 Satz 4 Nr. 3 des Telekommunikationsgesetzes vor Aufnahme des Betriebs der Telekommunikationsanlage oder vor Beginn des Angebots des Telekommunikationsdienstes nachzuweisen ist. Die Genehmigung kann in Fällen, in denen die Genehmigungsvoraussetzungen lediglich in wesentlichen Teilen, jedoch nicht vollständig erfüllt werden, mit Nebenbestimmungen, insbesondere mit Auflagen zur Nachbesserung oder mit einer Befristung, versehen werden. Für bauartgleiche technische Einrichtungen erteilt die Regulierungsbehörde für Telekommunikation und Post dem Antragsteller lediglich eine Genehmigung.

(5) Reichen die Unterlagen für die Prüfung nach Absatz 4 Satz 3 nicht aus, so gibt die Regulierungsbehörde für Telekommunikation und Post dem Antragsteller Gelegenheit, die Unterlagen innerhalb einer angemessenen Frist nachzubessern oder zu ergänzen. Die Frist nach § 88 Abs. 2 Satz 5 des Telekommunikationsgesetzes beginnt mit Vorlage des

Antrags nach Absatz 2 und der zugehörigen Unterlagen nach Absatz 3 bei der Regulierungsbehörde für Telekommunikation und Post, in den Fällen des Satzes 1 mit Vorlage der nachgebesserten oder ergänzten Unterlagen.

(6) Die Regulierungsbehörde für Telekommunikation und Post soll 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 angemessenen Frist zuleiten. Die rechtzeitig eingegangenen Stellungnahmen sind bei der Entscheidung über die Genehmigung zu berücksichtigen.

§ 19
Abnahme

(1) Zur Einleitung des gemäß § 88 Abs. 2 Satz 4 Nr. 3 des Telekommunikationsgesetzes vorgesehenen Abnahmeverfahrens hat der Verpflichtete der Regulierungsbehörde für Telekommunikation und Post im Rahmen der Anzeige nach § 88 Abs. 2 Satz 4 Nr. 2 des Telekommunikationsgesetzes eine Beschreibung der zur Umsetzung von Überwachungsmaßnahmen tatsächlich geschaffenen technischen Einrichtungen vorzulegen sowie etwaige Abweichungen von der technischen Gestaltung, die der Genehmigung zugrunde gelegen hat, darzulegen.

(2) Für die Abnahme nach Absatz 1, zu der die Regulierungsbehörde für Telekommunikation und Post auch Vertreter der in § 18 Abs. 6 genannten Stellen hinzuziehen kann, kann die Regulierungsbehörde für Telekommunikation und Post nach § 88 Abs. 2 Satz 4 Nr. 3 des Telekommunikationsgesetzes von dem Verpflichteten verlangen, dass er unentgeltlich

1. ihren Bediensteten die Durchführung der erforderlichen Messungen und Prüfungen einschließlich der Prüfung der Einhaltung der §§ 5, 6 und 7 Abs. 1 bis 4, der §§ 8 bis 10, 12 und 13 Satz 1, des § 14 Abs. 1, 2 Satz 1 bis 4 und Abs. 3, der §§ 16 und 17 Abs. 1 Satz 1 und 2 sowie der Technischen Richtlinie nach § 11 ermöglicht, wobei die zulässigen Abweichungen gemäß § 21 oder § 22 und die Übergangsfristen gemäß § 26 berücksichtigt werden,
2. bei Arbeiten nach Nummer 1 im erforderlichen Umfang mitwirkt und
3. die für die Arbeiten nach Nummer 1 erforderlichen Anschlüsse seiner Telekommunikationsanlage sowie die notwendigen Endgeräte bereitstellt, wenn diese Endgeräte bei der Regulierungsbehörde für Telekommunikation und Post nicht vorhanden sind.

(3) Entsprechen die zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen der Genehmigung, erteilt die Regulierungsbehörde für Telekommunikation und Post den Abnahmebescheid. Für bauartgleiche technische Einrichtungen erfolgt die Abnahme aufgrund einer Bauartprüfung. Weichen die zur

Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen von der Genehmigung ab, prüft die Regulierungsbehörde für Telekommunikation und Post, ob eine Änderungsgenehmigung erteilt werden kann. Im Falle genehmigungsfähiger Abweichungen erteilt die Regulierungsbehörde für Telekommunikation und Post den Abnahmebescheid unter gleichzeitiger Änderung der Genehmigung. Kann eine Änderungsgenehmigung nach Satz 4 nicht erteilt werden, kann die Regulierungsbehörde für Telekommunikation und Post

1. bei geringfügigen Abweichungen die Abnahme unter der Auflage erteilen, die Abweichungen innerhalb einer angemessenen Frist zu beseitigen, oder
2. bei wesentlichen Abweichungen die Abnahme im Benehmen mit den Stellen nach § 18 Abs. 6 unter der aufschiebenden Bedingung erteilen, die Abweichungen innerhalb einer angemessenen Frist zu beseitigen.

Bei Abweichungen, die eine Verletzung des Fernmeldegeheimnisses oder wesentliche Mängel bei der Überwachung zu Folge haben, hat die Regulierungsbehörde für Telekommunikation und Post die Abnahme auf diejenigen Dienste oder Dienstmerkmale zu beschränken, bei denen sich diese Mängel nicht auswirken.

§ 20
Änderungen der Telekommunikationsanlage, nachträglich festgestellte Mängel

Die §§ 18 und 19 gelten sinngemäß bei jeder Änderung der Telekommunikationsanlage oder eines mittels dieser Telekommunikationsanlage angebotenen Telekommunikationsdienstes, sofern diese Änderung Einfluss auf die Überwachungsfunktionalitäten hat. Für Prüfungen und Messungen, die die Regulierungsbehörde für Telekommunikation und Post im Falle von nachträglich aufgetretenen Mängeln durchführt, gilt § 19 Abs. 2 und 3 entsprechend.

Teil 5
Zulässige Abweichungen, Ausnahmeregelungen

§ 21
Abweichungen für Betreiber kleiner Telekommunikationsanlagen

(1) Für Betreiber von Telekommunikationsanlagen, an die nicht mehr als 10.000 Teilnehmer angeschlossen sind, sind auf Antrag des Verpflichteten Abweichungen von den Vorschriften dieser Verordnung entsprechend den Absätzen 2 bis 4 genehmigungsfähig, sofern diese Telekommunikationsanlage nicht Teil einer größeren Telekommunikationsanlage desselben Betreibers ist. § 5 Abs. 2 bleibt unberührt.

(2) Abweichend von § 6 Abs. 1 hat der Verpflichtete nach Absatz 1 sicherzustellen, dass er eine Überwachung innerhalb von 24 Stunden nach der Benachrichtigung technisch umsetzen kann.

(3) Der Verpflichtete nach Absatz 1 kann die zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen abweichend von § 8 Abs. 2 Satz 1 Nr. 6 und 7 und § 9 Abs. 1 so gestalten, dass

1. die Übermittlung der Kopie der zu überwachenden Telekommunikation an die berechtigte Stelle mit einem durch eine Pufferung bedingten Zeitversatz erfolgt, der bis zum Freiwerden vorhandener Übermittlungsressourcen andauern darf, oder
2. er der berechtigten Stelle die Kopie der zu überwachenden Telekommunikation am Ort der Telekommunikationsanlage zur Aufzeichnung übergibt.

(4) Abweichend von § 12 Abs. 1 Satz 1 bis 3 hat der Verpflichtete nach Absatz 1 sicherzustellen, dass er

1. innerhalb seiner üblichen Geschäftszeiten jederzeit über das Vorliegen einer Anordnung und die Dringlichkeit ihrer Umsetzung benachrichtigt werden und eine Anordnung entgegennehmen kann sowie
2. außerhalb seiner üblichen Geschäftszeiten innerhalb von 24 Stunden über das Vorliegen einer Anordnung und die Dringlichkeit ihrer Umsetzung benachrichtigt werden und eine Anordnung innerhalb von 24 Stunden nach der Benachrichtigung im Geltungsbereich dieser Verordnung entgegennehmen kann.

§ 22
Abweichungen auf Antrag, Feldversuche, Probebetriebe

(1) Die Regulierungsbehörde für Telekommunikation und Post kann im Rahmen der Genehmigung nach § 88 Abs. 2 Satz 1 des Telekommunikationsgesetzes im Benehmen mit den in § 18 Abs. 6 genannten Stellen auf Antrag eines Verpflichteten bei einzelnen Telekommunikationsanlagen hinsichtlich der Gestaltung der technischen Einrichtungen Abweichungen von einzelnen Bestimmungen dieser Rechtsverordnung oder von einzelnen Anforderungen der Technischen Richtlinie nach § 11 genehmigen, 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 der berechtigten Stellen nicht unverhältnismäßig hoch ist.

Der Antragsteller hat die Gründe für die Abweichungen nach Satz 1, die genaue Beschreibung des Übergabepunktes mit Hinweisen auf die Abweichungen von den Genehmigungsvoraussetzungen sowie die Folgen dieser Abweichungen der Regulierungsbehörde für Telekommunikation und Post mitzuteilen. Die

Regulierungsbehörde für Telekommunikation und Post ist unbeschadet möglicher Schutzrechtsvermerke des Antragstellers befugt, Mitteilungen nach Satz 2 an die in § 18 Abs. 6 genannten Stellen zu übermitteln, damit die bei den berechtigten Stellen vorhandenen Aufzeichnungseinrichtungen gegebenenfalls angepasst werden können. Die Genehmigung nach Satz 1 kann mit Nebenbestimmungen nach § 36 Abs. 2 des Verwaltungsverfahrensgesetzes versehen werden.

(2) Die Regulierungsbehörde für Telekommunikation und Post kann für die zur Umsetzung von Überwachungsmaßnahmen erforderlichen technischen Einrichtungen in 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 Telekommunikationsdienstleistungen dienen, eine befristete Genehmigung nach einem vereinfachten Verfahren erteilen. Sie kann dabei nach pflichtgemäßem Ermessen im Einzelfall vorübergehend auf die Einhaltung einzelner Anforderungen der Technischen Richtlinie nach § 11 verzichten, sofern

1. der Versuchs- oder Probebetrieb oder der Feldversuch der Telekommunikationsanlage für nicht länger als zwölf Monate vorgesehen ist,
2. nicht mehr als 10.000 Teilnehmer, 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 nicht unmöglich ist.

Absatz 1 Satz 2 bis 4 gilt sinngemäß.

Teil 6
Sonstige Vorschriften

§ 23
Mitwirkung bei Funktionsprüfungen der Aufzeichnungs- und Auswertungseinrichtungen

(1) Der Verpflichtete hat der berechtigten Stelle auf Verlangen Anschlüsse seiner Telekommunikationsanlage zu den üblichen Geschäftsbedingungen an den von diesen benannten Orten einzurichten und zu überlassen, damit die ordnungsgemäße Funktion der Aufzeichnungs- und Auswertungseinrichtungen geprüft werden kann. Der Verpflichtete hat die Überwachungsfunktionalitäten in Bezug auf diese Anschlüsse, über die ausschließlich zu Probezwecken erzeugte Telekommunikation ohne Beteiligung Dritter abgewickelt wird, erst anzuwenden nach schriftlicher Bestätigung der Regulierungsbehörde für Telekommunikation und Post. Darin sind der Zeitraum der Erprobung sowie die Rufnummer oder die mit der Rufnummer funktional vergleichbare Kennung des Anschlusses anzugeben, an den die zu erprobende Aufzeichnungseinrichtung angeschaltet ist.

(2) Absatz 1 Satz 1 und 2 gilt sinngemäß für Funktionsprüfungen, die die Regulierungsbehörde für Telekommunikation und Post im Rahmen der ihr gemäß § 88 Abs. 2 des Telekommunikationsgesetzes und der nach dieser Verordnung obliegenden Aufgaben wahrnimmt.

§ 24
Anforderungen an Anschlüsse für die berechtigte Stelle

(1) Die Anschlüsse für die berechtigte Stelle, an die diese ihre Aufzeichnungseinrichtungen anschaltet, hat der nach § 88 Abs. 4 des Telekommunikationsgesetzes verpflichtete Teilnehmernetzbetreiber 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 Abs. 2 vorzusehen.

(2) Der nach § 88 Abs. 4 des Telekommunikationsgesetzes verpflichtete Teilnehmernetzbetreiber hat im Störungsfall die unverzügliche Entstörung der Anschlüsse nach Absatz 1 sicherzustellen.

§ 25
Statistische Unterlagen

Die nach § 88 Abs. 5 Satz 1 des Telekommunikationsgesetzes zu erstellende Jahresstatistik ist nach der Anlage zu dieser Verordnung zu führen. Der Berichtszeitraum entspricht dem Kalenderjahr. Die Statistik ist der Regulierungsbehörde für Telekommunikation und Post spätestens zum 14. Februar des Folgejahres zu übermitteln. Abweichend von den Sätzen 2 und 3 können die Betreiber der in § 2 Abs. 2 genannten Telekommunikationsanlagen ihrer gesetzlichen Verpflichtung zur Erstellung einer Jahresstatistik über die durchgeführten Überwachungsmaßnahmen dadurch nachkommen, dass sie die erforderlichen Angaben nicht erst zu Beginn des folgenden Kalenderjahres, sondern bereits zum Abschluss der jeweiligen Überwachungsmaßnahme der Regulierungsbehörde für Telekommunikation und Post übermitteln.

Teil 7
Übergangsvorschriften, Schlussbestimmungen

§ 26
Übergangsvorschriften

(1) Soweit zur Umsetzung von Überwachungsmaßnahmen erforderliche technische Einrichtungen durch diese Rechtsverordnung erstmals vorgeschrieben werden oder durch

diese Rechtsverordnung geänderte Anforderungen an bestehende Einrichtungen gestellt werden, sind die entsprechenden technischen Einrichtungen unverzüglich, spätestens ab dem 1. Januar 2005 verfügbar zu halten.

(2) Bei den bestehenden Telekommunikationsanlagen für den Datenfunk oder für globale mobile Telekommunikation über geostationäre Satelliten sind die bestehenden technischen Abweichungen von den Vorschriften dieser Verordnung im Rahmen des zum Zeitpunkt des Inkrafttretens dieser Verordnung verfügbaren technischen Verfahrens bis zur Erneuerung der Systemtechnik, längstens jedoch bis zum 31. Dezember 2006 zulässig.

(3) Die Jahresstatistik nach § 25 ist erstmals für das Kalenderjahr 2001 zu erstellen.

§ 27
Inkrafttreten, Außerkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft. Gleichzeitig tritt die 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), außer Kraft.

Anlage
(zu § 25)

(U n t e r n e h m e n)

Jahresstatistik *für das* ***Kalenderjahr*** _____

über Maßnahmen zur Überwachung
der Telekommunikation nach den §§ 100a, 100b der Strafprozessordnung

Hinweise: 1. Für technische Ausprägungen von Telekommunikationsmöglichkeiten, die von dem Unternehmen nicht angeboten werden, sind die Zeilen 2.1 bis 2.7.X zu streichen.
2. Alle verbleibenden Zahlenfelder sind auszufüllen, daher bitte zutreffendenfalls ”0” einsetzen.

1.1 Anzahl der vorgelegten ***Anordnungen:*** ....._____
(sowohl von Richtern als auch von der Staatsanwaltschaft)-
- ***Verlängerungsanordnungen *)*** *und* ***Bestätigungen*** *gemäß § 100b Abs. 1 Satz 3 StPO bitte* ***nicht mitzählen*** -

1.2 Anzahl der vorgelegten ***Verlängerungsanordnungen *):*** ..... _____

2 Anzahl der in den Anordnungen benannten ***Kennungen:***

Lfd. Nr.	Technische Ausprägungen der Telekommunikationsmöglichkeiten, **Kennungen für:**	**Art der Anordnung**	
		”neue”Anordnungen (Nummer 1.1)	**Verlängerungsanordnungen** (Nummer 1.2)
2.1	Telefonanschlüsse (analog)	_____	_____
2.2	ISDN- Basisanschlüsse	_____	_____
2.3	ISDN-Primärmultiplex-Anschlüsse	_____	_____
2.4	Mobiltelefonanschlüsse	_____	_____
2.5	Funkrufanschlüsse	_____	_____
2.6	e-Mail	_____	_____
2.7	sonstige Ausprägungen (bitte Bezeichnung angeben)	_____	_____
2.7.1	_____	_____	_____

2.7.2 _____ _____ _____

2.7.X **(Für Angaben zu weiteren technischen Ausprägungen der Telekommunikationsmöglichkeiten bitte Zusatzblatt verwenden.)**

_____ _____

(Ort, Datum) (Unterschrift des Vertretungsberechtigten)

*) Anordnungen nach § 100b Abs. 2 Satz 5 der Strafprozessordnung (StPO).

II.3 Telekommunikations-Datenschutzverordnung (TDSV)

§ 1
Anwendungsbereich

(1) Diese Verordnung regelt den Schutz personenbezogener Daten der an der Telekommunikation Beteiligten bei der Erhebung, Verarbeitung und Nutzung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste 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) Soweit diese Verordnung oder andere besondere Rechtsvorschriften keine Regelungen enthalten, gelten die Vorschriften des Bundesdatenschutzgesetzes. Für geschlossene Benutzerkreise öffentlicher Stellen der Länder gilt die Verordnung mit der Maßgabe, dass an die Stelle des Bundesdatenschutzgesetzes die jeweiligen Landesdatenschutzgesetze treten.

§ 2
Begriffsbestimmungen

Im Sinne dieser Verordnung sind

1. Beteiligte an der Telekommunikation

a) die Vertragspartner (Kunden) bei Verträgen über Telekommunikationsdienste mit einem Diensteanbieter (Nummer 2) und

b) Personen, die Telekommunikationsdienste nutzen, die ein Diensteanbieter anbietet;

2. Diensteanbieter

alle, die ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken;

3. Bestandsdaten

personenbezogene Daten eines an der Telekommunikation Beteiligten, die erhoben werden, um ein Vertragsverhältnis über Telekommunikationsdienste einschließlich dessen inhaltlicher Ausgestaltung mit dem Diensteanbieter zu begründen oder zu ändern;

4. Verbindungsdaten

personenbezogene Daten eines an der Telekommunikation Beteiligten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden;

5. Kundenkarten

Karten, mit deren Hilfe Telekommunikationsverbindungen hergestellt und personenbezogene Daten erhoben werden können.

§ 3
Grundsätze

(1) Diensteanbieter dürfen für Telekommunikationszwecke personenbezogene Daten der an der Telekommunikation Beteiligten nur erheben, verarbeiten oder nutzen, soweit diese Verordnung oder andere Rechtsvorschriften es erlauben oder der Beteiligte eine Einwilligung erteilt hat, die den Vorschriften des Bundesdatenschutzgesetzes oder dieser Verordnung entspricht.

(2) Diensteanbieter dürfen die Erbringung von Telekommunikationsdiensten nicht von der Angabe personenbezogener Daten abhängig machen, die nicht erforderlich sind, um diese Dienste zu erbringen. Entsprechendes gilt für die Einwilligung des Beteiligten in die Verarbeitung oder Nutzung der Daten für andere Zwecke. Erforderlich können auch Angaben sein, die mit einem Telekommunikationsdienst in sachlichem Zusammenhang stehen.

(3) Diensteanbieter dürfen darüber hinaus im Zusammenhang mit der Erbringung von Telekommunikationsdiensten erhobene Daten für andere Zwecke nur verarbeiten oder nutzen, wenn eine andere Rechtsvorschrift eine solche Verwendung für diese Daten ausdrücklich vorsieht oder der Beteiligte eine Einwilligung erteilt hat, die den Vorschriften des Bundesdatenschutzgesetzes oder dieser Verordnung entspricht.

(4) Diensteanbieter haben sich an dem Ziel der Datenvermeidung und Datensparsamkeit auszurichten.

(5) Diensteanbieter haben ihre Kunden bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten so zu unterrichten, dass die Kunden in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Dabei sind die Kunden auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Beteiligten nach § 2 Nr. 1 Buchstabe b sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Das Auskunftsrecht nach dem Bundesdatenschutzgesetz bleibt davon unberührt.

(6) An ausländische Stellen dürfen Diensteanbieter personenbezogene Daten nach Maßgabe des Bundesdatenschutzgesetzes nur übermitteln, soweit es für die Erbringung von Telekommunikationsdiensten, für die Erstellung oder Versendung von Rechnungen oder für die Missbrauchsbekämpfung (§ 9 Abs. 1 Nr. 2) erforderlich ist.

§ 4
Einwilligung im elektronischen Verfahren

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

1. die Einwilligung auf einer eindeutigen und bewussten Handlung des Beteiligten beruht,

2. die Einwilligung protokolliert wird,

3. der Inhalt der Einwilligung jederzeit von dem Beteiligten abgerufen werden kann und

4. für einen Zeitraum von mindestens einer Woche ab Zugang der Erklärung eine Rücknahmemöglichkeit vorgesehen ist.

Das Recht der Beteiligten, die Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen, bleibt unberührt.

§ 5
Vertragsverhältnisse

(1) Der Diensteanbieter darf Bestandsdaten erheben, verarbeiten und nutzen, soweit dieses zur Erreichung des in § 2 Nr. 3 genannten Zweckes erforderlich ist. Im

Rahmen eines Vertragsverhältnisses mit einem anderen Diensteanbieter darf der Diensteanbieter Bestandsdaten seiner Kunden und der Kunden des anderen Diensteanbieters erheben, verarbeiten und nutzen, soweit dies zur Erfüllung des Vertrages zwischen den Diensteanbietern erforderlich ist. Eine Übermittlung der Bestandsdaten an Dritte erfolgt, soweit nicht diese Verordnung oder ein Gesetz sie zulässt, nur mit Einwilligung des an der Telekommunikation Beteiligten.

(2) Der Diensteanbieter darf die Bestandsdaten seiner Kunden und der Kunden seiner Diensteanbieter zur Beratung der Kunden, zur Werbung und zur Marktforschung nur verarbeiten und nutzen, soweit dies für diese Zwecke erforderlich ist und der Kunde eingewilligt
hat.

(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 Kunden erforderlich ist. Er kann von dem Ausweis eine Kopie erstellen. Die Kopie ist vom Diensteanbieter unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Kunden zu vernichten. Andere als die nach Absatz 1 zulässigen Daten darf der Diensteanbieter dabei nicht verarbeiten.

§ 6
Telekommunikationsverbindungen

(1) Der Diensteanbieter darf folgende Verbindungsdaten (§ 2 Nr. 4) erheben, verarbeiten und nutzen, soweit dies für die in dieser Verordnung genannten Zwecke erforderlich ist:

1. die Nummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortkennung;

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

3. den vom Kunden in Anspruch genommenen Telekommunikationsdienst;

4. die Endpunkte von festgeschalteten Verbindungen sowie ihren Beginn und ihr Ende nach Datum und Uhrzeit;

5. sonstige zum Aufbau und zur Aufrechterhaltung sowie zur Entgeltabrechnung notwendige Verbindungsdaten.

(2) Die gespeicherten Verbindungsdaten dürfen über das Ende der Verbindung hinaus nur verarbeitet oder genutzt werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 7, 8, 9 und 10 genannten Zwecke erforderlich sind. Im übrigen sind Verbindungsdaten vom Diensteanbieter spätestens am Tag nach Beendigung der Verbindung unverzüglich zu löschen.

(3) Diensteanbieter dürfen Verbindungsdaten nur mit Einwilligung des Anrufenden auch zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten verarbeiten und nutzen. Hierbei sind die Daten des Angerufenen unverzüglich zu anonymisieren. Eine zielnummernbezogene Verarbeitung und Nutzung der Verbindungsdaten durch den Diensteanbieter zu dem in Satz 1 genannten Zweck ist nur mit Einwilligung des Angerufenen zulässig. Hierbei sind die Daten des Anrufenden unverzüglich zu anonymisieren.

§ 7
Entgeltermittlung und Entgeltabrechnung

(1) Diensteanbieter dürfen einander die in § 6 Abs. 1 aufgeführten Verbindungsdaten übermitteln und nutzen, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Kunden benötigt werden. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er diesem 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 § 85 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120), das zuletzt gemäß Artikel 2 Abs. 6 des Gesetzes vom 26. August 1998 (BGBl. I S. 2521) geändert worden ist und der §§ 3, 5, 6, 7, 8 und 9 dieser Verordnung zu verpflichten.

(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 5 erheben und verarbeiten:

1. die Verbindungsdaten gemäß § 6 Abs. 1;

2. die Anschrift des Kunden 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 Verbindungsdaten nach § 6 Abs. 1 Nr. 1 bis 3 und Nr. 5 unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Nicht erforderliche Daten sind unverzüglich zu löschen. Die Verbindungsdaten dürfen unter Kürzung der Zielnummer um die letzten drei Ziffern zu Beweiszwecken für die Richtigkeit der berechneten Entgelte – vorbehaltlich des Absatzes 4 – höchstens sechs Monate nach Versendung der Rechnung gespeichert werden. Abweichend von Satz 3 darf die 0190er- oder 0900er Mehrwertdiensterufnummer ungekürzt gespeichert werden. Hat der Kunde gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 3 Einwendungen erhoben, dürfen die Verbindungsdaten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

(4) Auf Verlangen des Kunden hat der rechnungstellende Diensteanbieter die bei ihm gespeicherten Verbindungsdaten

1. vollständig zu speichern oder

2. mit Versendung der Rechnung an den Kunden vollständig zu löschen.

Soweit ein Kunde zur vollständigen oder teilweisen Übernahme der Entgelte für bei seinem Anschluss ankommende Verbindungen verpflichtet ist, steht ihm das Wahlrecht nach Nummer 1 nicht zu. Die Sätze 1 und 2 gelten nicht für

Diensteanbieter, die als Anbieter geschlossener Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

(5) Soweit es für die Abrechnung des Diensteanbieters mit anderen Diensteanbietern oder mit deren Kunden sowie anderer Diensteanbieter mit ihren Kunden erforderlich ist, darf der Diensteanbieter Verbindungsdaten speichern und übermitteln.

(6) 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 Verbindungsdaten übermitteln, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Kunden erforderlich sind.

§ 8
Einzelverbindungsnachweis

(1) Dem Kunden sind die nach § 7 Abs. 3 Satz 3 und Abs. 4 bis zur Versendung der Rechnung gespeicherten Daten derjenigen Verbindungen, für die er entgeltpflichtig ist**,** nur dann mitzuteilen, wenn er vor dem maßgeblichen Abrechnungszeitraum schriftlich eine aufgeschlüsselte Rechnung verlangt hat (Einzelverbindungsnachweis). Bei Anschlüssen im Haushalt ist die Mitteilung nur zulässig, wenn der Kunde schriftlich erklärt hat, dass er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber informiert hat und künftige Mitbenutzer unverzüglich darüber informiert werden, dass ihm die Verbindungsdaten zur Erteilung des Nachweises bekanntgegeben werden. Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Kunde schriftlich 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 oder eine solche Beteiligung nicht erforderlich ist. Soweit die öffentlich-rechtlichen Religionsgesellschaften für ihren Bereich eigene Mitarbeitervertreterregelungen erlassen haben, findet Satz 3 mit der Maßgabe Anwendung, dass an die Stelle des Betriebsrates oder der Personalvertretung die jeweilige Mitarbeitervertretung tritt. Dem Kunden dürfen darüber hinaus die nach § 7 Abs. 3 Satz 3 und 4 nach dem Versand der Rechnung gespeicherten Daten mitgeteilt werden, wenn er Einwendungen gegen die Höhe der Verbindungsentgelte erhoben hat. Soweit ein Kunde zur vollständigen oder teilweisen Übernahme der Entgelte für bei seinem Anschluss ankommende Verbindungen verpflichtet ist, dürfen ihm in dem für ihn bestimmten Einzelverbindungsnachweis die Nummern der anrufenden Anschlüsse nur unter Kürzung um die letzten drei Ziffern mitgeteilt werden. Satz 6 gilt 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 von Anschlüssen 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 Regulierungsbehörde für Telekommunikation und Post die Inhaber der angerufenen Anschlüsse in eine Liste aufgenommen hat. Der Beratung im Sinne des Satzes 1 dienen neben den in § 203 Abs. 1 Nr. 4 und Nr. 4a des Strafgesetzbuches genannten Personengruppen insbesondere die Telefonseelsorge und die Gesundheitsberatung. Die Regulierungsbehörde für Telekommunikation und Post nimmt die Inhaber der Anschlüsse auf Antrag in die Liste auf, wenn diese 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 den Inhalt der 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 (§ 2 Nr. 5) muss auch auf der Karte ein deutlicher Hinweis auf die mögliche Mitteilung der gespeicherten Verbindungsdaten ersichtlich sein. Sofern ein solcher Hinweis auf der Karte aus technischen Gründen nicht möglich oder für den Kartenemittenten unzumutbar ist, muss der Kunde eine Erklärung nach Absatz 1 Satz 2 oder 3 abgegeben haben.

§ 9
Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) Soweit es im Einzelfall erforderlich ist, darf der Diensteanbieter

1. zum Erkennen, Eingrenzen und Beseitigen von Störungen und Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verbindungsdaten der Beteiligten erheben, verarbeiten und nutzen;

2. bei Vorliegen schriftlich zu dokumentierender tatsächlicher Anhaltspunkte die Bestands- und Verbindungsdaten erheben, verarbeiten und nutzen, die zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und –dienste erforderlich sind.

(2) Der Diensteanbieter darf zu dem in Absatz 1 Nr. 2 genannten Zweck die erhobenen Verbindungsdaten in der Weise verarbeiten und nutzen, dass aus dem Gesamtbestand aller Verbindungsdaten, 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. Insbesondere darf der Diensteanbieter aus den nach Absatz 1 Nr. 2 erhobenen Verbindungsdaten und den Bestandsdaten seiner Kunden einen Gesamtdatenbestand bilden, der in pseudonymisierter Form Aufschluss über die von den einzelnen Kunden erzielten Umsätze gibt und unter Zugrundelegung geeigneter Missbrauchskriterien das Auffinden solcher Verbindungen des Netzes ermöglicht, bei denen der Verdacht einer Leistungserschleichung besteht. Die Daten der anderen Verbindungen sind unverzüglich zu löschen.

(3) Die Regulierungsbehörde für Telekommunikation und Post und der Bundesbeauftragte für den Datenschutz sind über Einführung und Änderung des Verfahrens nach Absatz 2 Satz 1 unverzüglich in Kenntnis zu setzen.

(4) In den Fällen des Absatzes 1 Nr. 2 darf im Einzelfall der Diensteanbieter Steuersignale erheben, verarbeiten und nutzen, soweit dies zum Aufklären und Unterbinden der dort genannten Handlungen unerlässlich ist. Die Regulierungsbehörde für Telekommunikation und Post ist hierüber in Kenntnis zu setzen. Im Übrigen gilt § 89 Abs. 3 Satz 3 und 4 sowie Abs. 4 und 5 des Telekommunikationsgesetzes.

§ 10
Mitteilen ankommender Verbindungen

(1) Trägt ein Kunde 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 Anschlüsse zu erteilen, von denen die Anrufe ausgehen. Die Auskunft darf sich nur auf Anrufe beziehen, die nach dem Antrag durchgeführt werden. Der Diensteanbieter darf die Nummern, Namen und Anschriften der Inhaber dieser Anschlüsse sowie

Datum und Uhrzeit des Beginns der Verbindungen und der Verbindungsversuche erheben, speichern und seinem Kunden mitteilen. Die Sätze 1 bis 3 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

(2) Die Bekanntgabe nach Absatz 1 Satz 3 darf nur erfolgen, wenn der Kunde zuvor die Verbindungen nach Datum, Uhrzeit oder anderen geeigneten Kriterien eingrenzt, soweit ein Missbrauch der Überwachungsmöglichkeit nicht auf andere Weise ausgeschlossen werden kann. Sind die Inhaber der genannten Anschlüsse nicht in einem öffentlichen Kundenverzeichnis nach § 13 eingetragen, dürfen dem Kunden lediglich Namen und Anschriften der Anschlussinhaber mitgeteilt werden.

(3) Im Fall einer netzübergreifenden Auskunft sind die an der Verbindung mitwirkenden anderen Diensteanbieter verpflichtet, dem Diensteanbieter des bedrohten oder belästigten Kunden die erforderlichen Auskünfte zu erteilen, sofern sie über diese Daten verfügen.

(4) Der Kunde des Anschlusses, von dem die festgestellten Verbindungen ausgegangen sind, ist zu unterrichten, dass über diese Auskunft gegeben wurde. Davon kann abgesehen werden, wenn der Antragsteller in schriftlicher Form schlüssig vorgetragen hat, dass ihm aus dieser Mitteilung wesentliche Nachteile entstehen können und diese Nachteile bei Abwägung mit den schutzwürdigen Interessen des Anrufers als wesentlich schwerwiegender erscheinen. Erhält der Kunde, 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 Regulierungsbehörde für Telekommunikation und Post sowie der Bundesbeauftragte für den Datenschutz sind über die Einführung und Änderung des Verfahrens zur Sicherstellung der Absätze 1 bis 4 unverzüglich in Kenntnis zu setzen.

§ 11
Anzeige der Nummer des Anrufers und des Angerufenen und deren Unterdrückung

(1) Bietet der Diensteanbieter die Anzeige der Nummer des Anrufers an, so müssen der Anrufende und der Angerufene die Möglichkeit haben, die Nummernanzeige dauernd oder für jeden Anruf einzeln auf einfache Weise und unentgeltlich zu unterdrücken. Der Angerufene muss die Möglichkeit haben, eingehende Anrufe, bei

denen die Nummernanzeige durch den Anrufenden unterdrückt wurde, auf einfache Weise und unentgeltlich abzuweisen. Der Diensteanbieter hat die Dienste nach Satz 1 und 2 nur insoweit anzubieten, als dies technisch möglich ist. Die Sätze 1 bis 3 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

(2) Auf Antrag des Kunden muss der Diensteanbieter Anschlüsse bereitstellen, bei denen die Übermittlung der Nummer des anrufenden Anschlusses an den angerufenen Anschluss unentgeltlich ausgeschlossen ist. Die Anschlüsse sind auf Antrag des Kunden in dem öffentlichen Kundenverzeichnis (§ 13 Abs. 1) seines Diensteanbieters entsprechend zu kennzeichnen. Ist eine Kennzeichnung nach Satz 2 erfolgt, so darf an den so gekennzeichneten Anschluss eine Übermittlung der Nummer des anrufenden Anschlusses erst dann erfolgen, wenn zuvor die Kennzeichnung in der aktualisierten Fassung des Kundenverzeichnisses nicht mehr enthalten ist.

(3) Hat der Kunde die Eintragung in das Kundenverzeichnis nicht nach § 13 Abs. 2 beantragt, unterbleibt die Anzeige seiner Nummer bei dem angerufenen Anschluss, es sei denn, dass der Kunde die Übermittlung seiner Nummer ausdrücklich wünscht.

(4) Wird die Anzeige der Nummer des Angerufenen angeboten, so muss der Angerufene die Möglichkeit haben, die Anzeige seiner Nummer beim Anrufenden auf einfache Weise und unentgeltlich zu unterdrücken, soweit dies technisch möglich ist. Absatz 1 Satz 4 gilt entsprechend.

(5) Die Absätze 1 und 4 gelten auch für Anrufe in das Ausland und für aus dem Ausland kommende Anrufe, soweit sie den Anrufer oder Angerufenen im Inland betreffen.

(6) Bei Einrichtungen, die Notrufe unter den Nummern 110, 112, 124124 beantworten oder bearbeiten, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Anzeige von Nummern der Anrufenden ausgeschlossen wird. Absatz 1 Satz 4 gilt entsprechend.

§ 12
Anrufweiterschaltung

Der Diensteanbieter ist verpflichtet, seinen Kunden 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.

§ 13
Öffentliche Kundenverzeichnisse

(1) Der Diensteanbieter darf öffentliche Verzeichnisse seiner Kunden in Form von Druckwerken oder elektronischen Verzeichnissen erstellen und herausgeben.

(2) Die Kunden 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 Kunden bestimmen, welche Angaben in den Verzeichnissen veröffentlicht werden sollen, dass die Eintragung nur in gedruckten oder elektronischen Verzeichnissen erfolgt oder dass jegliche Eintragung unterbleibt. Die Eintragungen sind gesondert zu kennzeichnen. Auf Verlangen des Kunden dürfen Mitbenutzer eingetragen werden, soweit diese damit einverstanden sind.

§ 14
Auskunftserteilung

(1) Der Diensteanbieter darf im Einzelfall Auskunft über die in öffentlichen Kundenverzeichnissen enthaltenen Rufnummern erteilen oder durch Dritte erteilen lassen (Telefonauskunft). Die Übertragung der Auskunftserteilung an Dritte ist nur zulässig, wenn der Diensteanbieter den Dritten verpflichtet, die Daten nur zur Auskunft zu verarbeiten und zu nutzen und die Beschränkungen des § 13 und der Absätze 2 und 3 einzuhalten.

(2) Die Telefonauskunft über Rufnummern von Kunden 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 § 13 Abs. 2 veröffentlichte Daten dürfen nur erteilt werden, wenn der Kunde mit einer weitergehenden Auskunftserteilung einverstanden ist.

(3) Ein Widerspruch nach Absatz 2 Satz 1 oder ein Einverständnis nach Absatz 2 Satz 2 sind in den Verzeichnissen des Diensteanbieters unverzüglich zu vermerken. Er ist auch von den anderen Diensteanbietern zu beachten, sobald diese in

zumutbarer Weise Kenntnis darüber erlangen konnten, dass der Widerspruch in den Verzeichnissen des Diensteanbieters vermerkt ist.

(4) Die Auskunftserteilung über Namen und andere Daten von Kunden, von denen nur die Rufnummer bekannt ist, ist unzulässig.

§ 15
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 Kunden 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 Kunden 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 erfordern.

§ 16
Nachrichtenübermittlungssysteme mit Zwischenspeicherung

(1) Der Diensteanbieter darf bei Diensten, für deren Durchführung eine Zwischenspeicherung erforderlich ist, Nachrichteninhalte, insbesondere Sprach-, Ton-, Text- und Grafikmitteilungen von Kunden, 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 Kunden oder durch Eingabe des Kunden in Telekommunikationsanlagen anderer Diensteanbieter weitergeleitet.

2. Ausschließlich der Kunde bestimmt durch seine Eingabe Inhalt, Umfang und Art der Verarbeitung.

3. Ausschließlich der Kunde bestimmt, wer Nachrichteninhalte eingeben und darauf zugreifen darf (Zugriffsberechtigter).

4. Der Diensteanbieter darf dem Kunden mitteilen, dass der Empfänger auf die Nachricht zugegriffen hat.

5. Der Diensteanbieter darf Nachrichteninhalte nur entsprechend dem mit dem Kunden geschlossenen Vertrag löschen.

(2) Der Diensteanbieter hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um Fehlerübermittlungen 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.

§ 17
Ordnungswidrigkeiten

Ordnungswidrig im Sinne des § 96 Abs. 1 Nr. 9 des Telekommunikationsgesetzes handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 5 Abs. 2 Bestandsdaten verarbeitet oder nutzt,

2. entgegen § 6 Abs. 2 Satz 1 oder Abs. 3 Satz 1 oder 3 Verbindungsdaten verarbeitet oder nutzt,

3. entgegen § 6 Abs. 2 Satz 2 oder § 7 Abs. 3 Satz 2 Daten nicht oder nicht rechtzeitig löscht oder

4. entgegen § 15 Abs. 2 Satz 2 Daten oder Belege nicht oder nicht rechtzeitig löscht.

§ 18
Inkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft. Gleichzeitig tritt die Telekommunikationsdienstunternehmen-Datenschutzverordnung vom 12. Juli 1996 (BGBl. I S. 982) außer Kraft.

II.4 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.1002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

Aus redaktionellen Gründen wurde die Datenschutzrichtlinie am Ende dieser Ausgabe angefügt.

II.5 Telekommunikations-Kundenschutzverordnung (TKV)

Erster Teil
Allgemeine Bestimmungen

§ 1
Anwendungsbereich

(1) Die Verordnung regelt die besonderen Rechte und Pflichten der Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit und derjenigen, die diese Leistungen vertraglich in Anspruch nehmen oder begehren (Kunden).

(2) Vereinbarungen, die zuungunsten des Kunden von dieser Verordnung abweichen, sind unwirksam.

§ 2
Nichtdiskriminierung

Marktbeherrschende Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit haben diese Leistungen jedermann zu gleichen Bedingungen zur Verfügung zu stellen, es sei denn, dass unterschiedliche Bedingungen sachlich gerechtfertigt sind.

X

X

X

§ 4
Angebote für Diensteanbieter

(1) Betreiber öffentlicher Telekommunikationsnetze haben ihr Leistungsangebot so zu gestalten, dass Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit diese Leistungen im eigenen Namen und auf eigene Rechnung vertreiben und ihren Kunden anbieten können. Dies gilt nicht, wenn die Verpflichtung im Einzelfall sachlich nicht gerechtfertigt ist. Die in Verleihungen nach § 97 Abs. 5 des Telekommunikationsgesetzes festgelegten entsprechenden Verpflichtungen bleiben unberührt.

(2) Der Netzbetreiber darf die Diensteanbieter weder ausschließlich noch unverhältnismäßig lange an sich binden, noch hinsichtlich ihrer eigenen Preis- und Konditionengestaltung oder hinsichtlich anderer Betätigungsfelder einschränken. Er

darf Diensteanbietern keine ungünstigeren Bedingungen einräumen als dem eigenen Vertrieb oder verbundenen Unternehmen, es sei denn, dass dies sachlich gerechtfertigt ist.

§ 5
Verbindungspreisberechnung

Bei der Abrechnung haben die Anbieter folgende Grundsätze zu beachten:

1. Die Dauer zeitabhängig tarifierter Verbindungen von Telekommunikationsdienstleistungen für die Öffentlichkeit ist unter regelmäßiger Abgleichung mit einem amtlichen Zeitnormal zu ermitteln.

2. Die Systeme, Verfahren und technischen Einrichtungen, mit denen die Umrechnung der nach Nummer 1 ermittelten Verbindungsdaten in Entgeltforderungen erfolgt, sind vom Anbieter einer regelmäßigen Kontrolle auf Abrechnungsgenauigkeit und Übereinstimmung mit den vertraglich vereinbarten Entgelten einschließlich der Verzonungsdaten zu unterziehen.

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

§ 6
Leistungseinstellungen

(1) Ein Unternehmen, dem nach § 19 des Telekommunikationsgesetzes die Erbringung von Universaldienstleistungen auferlegt ist oder das Leistungen nach § 97 Abs. 1 des Telekommunikationsgesetzes erbringt, darf diese Leistungen nur vorübergehend aufgrund grundlegender, in Übereinstimmung mit dem Recht der Europäischen Union stehenden Anforderungen einstellen oder beschränken. Es hat auf die Belange der Kunden Rücksicht zu nehmen und die Leistungseinstellungen

oder -beschränkungen im Rahmen der technischen Möglichkeiten auf den betroffenen Dienst zu beschränken.

(2) Grundlegende Anforderungen, die eine Beschränkung von Universaldienstleistungen rechtfertigen, sind

1. die Sicherheit des Netzbetriebes,

2. die Aufrechterhaltung der Netzintegrität, insbesondere die Vermeidung schwerwiegender Störungen des Netzes, der Software oder gespeicherter Daten,

3. die Interoperabilität der Dienste,

4. der Datenschutz.

(3) Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit haben bei längeren, vorübergehenden Leistungseinstellungen oder -beschränkungen die Kunden in geeigneter Form über Art, Ausmaß und Dauer der Leistungseinstellung zu unterrichten. Im Falle voraussehbarer Leistungseinstellungen oder -beschränkungen besteht zudem eine Verpflichtung zur vorherigen Unterrichtung gegenüber denjenigen Kunden, die auf eine ununterbrochene Verbindung oder einen jederzeitigen Verbindungsaufbau angewiesen sind und dies dem Anbieter unter Angabe von Gründen schriftlich mitgeteilt haben. Die Mitteilungspflicht über den Beginn der Einstellung besteht nicht, wenn die Unterrichtung

1. nach den Umständen objektiv nicht vorher möglich ist oder

2. die Beseitigung bereits eingetretener Unterbrechungen verzögern würde.

§ 7
Haftung

(1) Schadensersatz- und Unterlassungsansprüche der Kunden der Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit richten sich nach § 40 des Telekommunikationsgesetzes und den allgemeinen gesetzlichen Bestimmungen.

(2) Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit haften für Vermögensschäden bis zu einem Betrag von fünfundzwanzigtausend Deutsche Mark je Nutzer. Dies gilt nicht gegenüber Nutzern, die ihrerseits

Telekommunikationsdienstleistungen für die Öffentlichkeit erbringen. Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit können die Haftung für diese Leistungen im Verhältnis zueinander durch Vereinbarung der Höhe nach beschränken. Eine vertragliche Haftungsbegrenzung darf die Summe der Mindesthaftungsbeträge gegenüber den geschädigten Endkunden des anderen Nutzers nicht unterschreiten. Gegenüber der Gesamtheit der Geschädigten ist die Haftung des Anbieters auf zwanzig Millionen Deutsche Mark jeweils je schadenverursachendes Ereignis begrenzt. Übersteigen die Entschädigungen, die mehreren aufgrund desselben Ereignisses zu leisten sind, die Höchstgrenze, so wird der Schadensersatz in dem Verhältnis gekürzt, in dem die Summe aller Schadensersatzansprüche zur Höchstgrenze steht. Die Haftungsbegrenzung der Höhe nach entfällt, wenn der Schaden vorsätzlich verursacht wurde.

§ 8
Verjährung

Die vertraglichen Ansprüche der Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit und ihrer Kunden aus der Inanspruchnahme dieser Leistungen verjähren in zwei Jahren. § 201 des Bürgerlichen Gesetzbuches gilt entsprechend.

Zweiter Teil
Sprachkommunikationsdienstleistungen und Netzzugang

Erster Abschnitt
Allgemeine Bestimmungen

§ 9
Verfügbarkeit als Universaldienstleistung

(1) Soweit ein Unternehmen Sprachtelefondienst und die damit in unmittelbarem Zusammenhang stehenden Leistungen aufgrund einer Verpflichtung zum Universaldienst nach § 19 des Telekommunikationsgesetzes oder Leistungen nach § 97 Abs. 1 des Telekommunikationsgesetzes erbringt, hat der Kunde gegen dieses im Rahmen der Gesetze und der Allgemeinen Geschäftsbedingungen einen Anspruch auf die Erbringung der entsprechenden Leistungen. Der Netzzugang muss es dem Kunden ermöglichen, im Rahmen der Gesetze nationale und internationale Anrufe zu tätigen und zu empfangen, und zur Sprach-, Faksimile- und Datenkommunikation geeignet sein.

(2) Der Kunde kann den Vertrag mit seinem nicht zum Universaldienst verpflichteten Anbieter von Sprachtelefondienst ohne Einhaltung einer Frist kündigen, sofern der Anbieter dem Kunden Leistungen bereitstellt, die nicht dem Mindestkatalog der Telekommunikations-Universaldienstleistungsverordnung entsprechen, und er den Kunden bei Vertragsabschluss auf diesen Umstand nicht schriftlich hingewiesen hat.

§ 10
Grundstückseigentümererklärung

(1) Wer Zugänge zu öffentlichen Telekommunikationsnetzen anbietet, kann den Abschluss eines Vertrages über diese Leistungen davon abhängig machen, dass dem Netzbetreiber für das betroffene Grundstück eine Einverständniserklärung des dinglich Berechtigten vorgelegt wird (Grundstückseigentümererklärung, Anlage 1).

(2) Der Netzbetreiber stellt dem dinglich Berechtigten eine Gegenerklärung aus (Anlage 2).

(3) Soll ein Zugang zu einem öffentlichen Telekommunikationsnetz von einem anderen Anbieter bereitgestellt werden, so hat der Berechtigte einer Grundstückseigentümererklärung dem anderen Anbieter von Zugängen zu öffentlichen Telekommunikationsnetzen die Mitbenutzung der auf dem Grundstück und in den darauf befindlichen Gebäuden verlegten Leitungen und Vorrichtungen zu ermöglichen, sofern der Grundstückseigentümer keine weitere Grundstückseigentümererklärung erteilt und erforderliche Nutzungen des Berechtigten der Mitbenutzung nicht entgegenstehen. Er kann hierfür ein Entgelt erheben, das sich an den Kosten der effizienten Leistungsbereitstellung orientiert.

§ 11
Sicherheitsleistung

(1) Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit, denen nach § 19 des Telekommunikationsgesetzes die Erbringung von Universaldienstleistungen auferlegt ist, sind berechtigt, die Überlassung von Universaldienstleistungen an Endkunden von einer Sicherheitsleistung in angemessener Höhe abhängig zu machen, wenn zu befürchten ist, dass der Kunde seinen vertraglichen Verpflichtungen nicht oder nicht rechtzeitig nachkommt. Die Sicherheitsleistung kann durch Bürgschaftserklärung eines im Europäischen

Wirtschaftsraum zugelassenen Kreditinstituts erfolgen. Der Anbieter ist berechtigt, die Sicherheitsleistung auf eine solche Bürgschaftserklärung und die Hinterlegung von Geld zu beschränken. Die Sicherheitsleistung ist unverzüglich zurückzugeben oder zu verrechnen, sobald die Voraussetzungen für ihre Erbringung weggefallen sind.

(2) Als angemessen im Sinne des Absatzes 1 Satz 1 ist in der Regel ein Betrag in Höhe des Bereitstellungspreises zuzüglich des sechsfachen Grundpreises anzusehen. Eine Anforderung höherer Beträge ist gegenüber dem Kunden anhand der Umstände seines Einzelfalles zu begründen. Für die Festlegung der zu sichernden Forderungen kommen dabei insbesondere die Höhe der Zahlungsrückstände aus einem früheren Vertragsverhältnis über die Bereitstellung eines allgemeinen Netzzugangs oder von Sprachtelefondienst, das Telefonier- und Zahlungsverhalten des Kunden sowie objektive Anhaltspunkte für ein künftiges erhöhtes Aufkommen von Tarifeinheiten in Betracht.

(3) Die Sicherungsmöglichkeiten der Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit richten sich im übrigen nach den allgemeinen Gesetzen.

§ 12
Entstörungsdienst

Marktbeherrschende Anbieter von Sprachtelefondienst haben auf Verlangen des Kunden einer Störung unverzüglich, auch nachts und an Sonn- und Feiertagen, nachzugehen. Die vertraglichen Bedingungen für den Entstörungsdienst sind in die Allgemeinen Geschäftsbedingungen des Anbieters aufzunehmen.

§ 13
Allgemeiner Netzzugang

(1) Der allgemeine Zugang zu festen öffentlichen Telekommunikationsnetzen ist mit einer räumlich frei zugänglichen Schnittstelle zu versehen. Er ist an einer mit dem Kunden zu vereinbarenden geeigneten Stelle zu installieren. Hierbei sind die Normen und Schnittstellenspezifikationen zu beachten, auf die nach Artikel 5 Abs. 1 der Richtlinie 90/387/EWG des Rates vom 28. Juni 1990 zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung des offenen Netzzugangs (Open Network Provision - ONP) (ABl. EG Nr. L 192 S. 1 in der

Fassung von Artikel 1 Nr. 5 der Richtlinie 97/51/EG des Europäischen Parlaments und des Rates vom 6. Oktober 1997 zur Anpassung der Richtlinien 90/387/EWG und 92/44/EWG des Rates an ein wettbewerbsorientiertes Telekommunikationsumfeld (ABL. EG Nr. L 295, S. 23) im Amtsblatt der Europäischen Gemeinschaften verwiesen wird oder die nach Artikel 5 Abs. 3 in Verbindung mit Artikel 10 der genannten Richtlinie für verbindlich erklärt wurden.

(2) Der Kunde muss die Möglichkeit haben, im Rahmen des Sprachtelefondienstes die Nutzung seines Netzzugangs durch eine netzseitige Sperrung bestimmter Arten von Rufnummern zu beschränken.

(3) Der Kunde kann von einem marktbeherrschenden Anbieter von Sprachtelefondienst im Rahmen der technischen Durchführbarkeit verlangen, dass über den allgemeinen Netzzugang im Rahmen der datenschutzrechtlichen Bestimmungen die Anzeige der Teilnehmerrufnummer des Anrufenden und eine direkte Durchwahl möglich sind.

(4) Allgemeine Zugänge zu öffentlichen Telekommunikationsnetzen müssen die Möglichkeit des Zugangs zu Vermittlungs- und Unterstützungsdiensten sowie zu Auskunftsdiensten über Teilnehmerrufnummern eröffnen.

(5) Wechselt der Kunde den Anbieter des allgemeinen Netzzugangs zu einem öffentlichen Telekommunikationsnetz, so kann die Kündigung durch den neuen Anbieter entgegengenommen und dem alten Anbieter übermittelt werden.

Zweiter Abschnitt
Rechnungserteilung und Einwendungen

§ 14
Einzelverbindungsnachweis

Verlangt der Kunde für Sprachkommunikationsdienstleistungen für die Öffentlichkeit vor dem maßgeblichen Abrechnungszeitraum eine nach Einzelverbindungen aufgeschlüsselte Rechnung, so hat der Anbieter im Rahmen der technischen Möglichkeiten und der datenschutzrechtlichen Vorschriften diesen Einzelverbindungsnachweis zu erteilen. Dies gilt nicht, wenn nach der besonderen Art der Leistung eine Rechnung üblicherweise nicht erteilt wird. Der Einzelverbindungsnachweis muss im Rahmen der datenschutzrechtlichen Bestimmungen die Entgelte so detailliert ausweisen, dass die Überprüfung und

Kontrolle der entstandenen Entgeltforderungen möglich ist. Die Standardform des Einzelverbindungsnachweises ist unentgeltlich zur Verfügung zu stellen.

§ 15
Rechnungserstellung

(1) Soweit der Kunde mit anderen Anbietern von Telekommunikationsdienstleistungen für die Öffentlichkeit nicht etwas anderes vereinbart, ist ihm von seinem Anbieter des Zugangs zum öffentlichen Telekommunikationsnetz (Rechnungsersteller) eine Rechnung zu erstellen, die auch die Entgelte für Verbindungen ausweist, die durch Auswahl anderer Anbieter von Netzdienstleistungen über den Netzzugang des Kunden entstehen. Die Rechnung muss die einzelnen Anbieter und zumindest die Gesamthöhe der auf sie entfallenden Entgelte erkennen lassen. § 14 bleibt unberührt. Die Zahlung an den Rechnungsersteller hat befreiende Wirkung auch gegenüber den anderen auf der Rechnung aufgeführten Anbietern. Zum Zwecke der Durchsetzung der Forderungen gegenüber ihren Kunden hat der Rechnungsersteller den anderen Anbietern die erforderlichen Bestands- und Verbindungdaten zu übermitteln.

(2) Begleicht der Kunde die Rechnung nur teilweise, ist, soweit nichts anderes vereinbart ist, im Zweifel davon auszugehen, dass die Zahlung auf die Forderungen der einzelnen Anbieter entsprechend ihrem Anteil an der Gesamtforderung erfolgt.

§ 16
Nachweis der Entgeltforderungen

(1) Erhebt der Kunde bei Telekommunikationsdienstleistungen für die Öffentlichkeit, die auf den für die Sprachkommunikation für die Öffentlichkeit vorgesehenen Telekommunikationsnetzen erbracht werden, Einwendungen gegen die Höhe der ihm in Rechnung gestellten Verbindungsentgelte, so ist das Verbindungsaufkommen unter Wahrung des Schutzes der Mitbenutzer auch ohne Auftrag zur Erteilung eines Einzelentgeltnachweises nach den einzelnen Verbindungsdaten aufzuschlüsseln und eine technische Prüfung durchzuführen, deren Dokumentation dem Kunden auf Verlangen vorzulegen ist.

(2) Soweit aus technischen Gründen oder auf Wunsch des Kunden keine Verbindungsdaten gespeichert oder gespeicherte Verbindungsdaten auf Wunsch des Kunden oder auf Grund rechtlicher Verpflichtung gelöscht wurden, trifft den Anbieter

keine Nachweispflicht für die Einzelverbindungen, wenn der Kunde in der Rechnung auf die nach den gesetzlichen Bestimmungen geltenden Fristen für die Löschung gespeicherter Verbindungsdaten in drucktechnisch deutlich gestalteter Form hingewiesen wurde. Soweit eine Speicherung aus technischen Gründen nicht erfolgt, entfällt die Nachweispflicht, wenn der Kunde vor der Rechnungserteilung auf diese Beschränkung der Möglichkeiten des Anschlusses in drucktechnisch deutlich gestalteter Form hingewiesen wurde.

(3) Dem Anbieter obliegt der Nachweis, die Leistung bis zu der Schnittstelle, an der der allgemeine Netzzugang dem Kunden bereitgestellt wird, technisch einwandfrei erbracht und richtig berechnet zu haben. Ergibt die technische Prüfung Mängel, die die beanstandete Entgeltermittlung beeinflusst haben könnten, wird widerleglich vermutet, dass die Verbindungsentgelte des Anbieters unrichtig ermittelt sind. Ist der Nachweis erbracht, dass der Netzzugang in vom Kunden nicht zu vertretendem Umfang genutzt wurde, oder rechtfertigen Tatsachen die Annahme, dass die Höhe der Verbindungsentgelte auf Manipulationen Dritter an öffentlichen Telekommunikationsnetzen zurückzuführen ist, ist der Anbieter nicht berechtigt, die betreffenden Verbindungsentgelte vom Kunden zu fordern.

§ 17
Entgeltermittlung bei unklarer Forderungshöhe

Ist davon auszugehen, dass für Verbindungen berechnete Entgeltforderungen unrichtig sind, ohne dass ihre richtige Höhe feststellbar ist, so wird für die Abrechnung die durchschnittliche Entgeltforderung des jeweiligen Anbieters aus den unbeanstandet gebliebenen sechs zurückliegenden Abrechnungszeiträumen zugrundegelegt. Das gilt auch, wenn nach den Umständen erhebliche Zweifel bleiben, ob der allgemeine Netzzugang des Kunden im Umfang der Entgeltforderungen in einer dem Kunden zurechenbaren Weise in Anspruch genommen wurde. Ist die Zeit der Überlassung des allgemeinen Netzzugangs durch den Anbieter kürzer als sechs Abrechnungszeiträume, so wird die Anzahl der vorhandenen Abrechnungszeiträume zugrunde gelegt. Bei der Durchschnittsberechnung sind die tatsächlichen Verhältnisse zu berücksichtigen. Wenn in den entsprechenden Abrechnungszeiträumen der Vorjahre bei vergleichbaren Umständen niedrigere Entgeltforderungen angefallen sind, als sich bei der Durchschnittsberechnung ergeben würde, treten diese Entgeltforderungen an die Stelle der berechneten Entgeltforderungen. Danach zuviel gezahlte Entgelte werden erstattet. Dem Kunden bleibt der Nachweis vorbehalten, dass der Netzzugang in dem entsprechenden Abrechnungszeitraum gar nicht genutzt wurde.

§ 18
Kundenvorgabe der Entgelthöhe

Ab dem 1. Januar 2001 kann der Kunde gegenüber dem Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit vorgeben, bis zu welcher monatlichen Entgelthöhe er die Dienstleistung in Anspruch nehmen will. Der Anbieter muss sicherstellen, dass diese Entgelthöhe nicht ohne Zustimmung des Kunden überschritten wird.

§ 19
Sperre; Zahlungsverzug

(1) Anbieter allgemeiner Zugänge zu festen öffentlichen Telekommunikationsnetzen und Anbieter von Sprachtelefondienst sind berechtigt, die Inanspruchnahme dieser Leistungen ganz oder teilweise zu unterbinden (Sperre), wenn der Kunde

1. mit Zahlungsverpflichtungen von mindestens einhundertfünfzig Deutsche Mark in Verzug ist und eine geleistete Sicherheit verbraucht ist oder

2. ein Grund zur Sperre nach Absatz 2 besteht.

(2) Sperren dürfen frühestens zwei Wochen nach schriftlicher Androhung und unter Hinweis auf die Möglichkeit des Kunden, Rechtsschutz vor den Gerichten zu suchen, durchgeführt werden. Die Androhung der Sperre kann mit der Mahnung verbunden werden. Eine Sperre ohne Ankündigung und Einhaltung einer Wartefrist ist nur zulässig, wenn

1. der Kunde Veranlassung zu einer fristlosen Kündigung des Vertragsverhältnisses gegeben hat oder

2. eine Gefährdung der Einrichtungen des Anbieters, insbesondere des Netzes, durch Rückwirkungen von Endeinrichtungen oder eine Gefährdung der öffentlichen Sicherheit droht oder

3. das Entgeltaufkommen in sehr hohem Maße ansteigt und Tatsachen die Annahme rechtfertigen, dass der Kunde bei einer späteren Durchführung der Sperre Entgelte für in der Zwischenzeit erbrachte Leistungen nicht, nicht vollständig oder

nicht rechtzeitig entrichtet und geleistete Sicherheiten verbraucht sind und die Sperre nicht unverhältnismäßig ist.

(3) Sperren sind im Rahmen der technischen Möglichkeiten auf den betroffenen Dienst zu beschränken und unverzüglich aufzuheben, sobald die Gründe für ihre Durchführung entfallen sind. Eine Vollsperrung des allgemeinen Netzzugangs darf erst nach Durchführung einer mindestens einwöchigen Abgangssperre erfolgen.

(4) Die Sperre nach Absatz 1 Nummer 1 unterbleibt, wenn gegen die Rechnung begründete Einwendungen erhoben wurden und der Durchschnittsbetrag nach § 17 bezahlt oder eine Stundungsvereinbarung getroffen ist.

Dritter Abschnitt
Besondere Nebenleistungen

§ 20
Zuteilung von Teilnehmerrufnummern

(1) Soweit im Rahmen der Regelungen nach § 43 Abs. 2 des Telekommunikationsgesetzes eine Zuteilung von Teilnehmerrufnummern nicht durch die Regulierungsbehörde erfolgt, erhält der Kunde die benötigten Teilnehmerrufnummern von seinem Anbieter des Zugangs zum öffentlichen Telekommunikationsnetz schriftlich zugeteilt (abgeleitete Zuteilung). Die Zuteilung erfolgt aus den Rufnummernblöcken, die dem Betreiber des Telekommunikationsnetzes oder dem Anbieter von Telekommunikationsdienstleistungen von der Regulierungsbehörde zugeteilt wurden (originäre Zuteilung).

(2) Der Kunde hat Anspruch auf diskriminierungsfreie Zuteilung der Teilnehmerrufnummern im Rahmen der von der Regulierungsbehörde nach § 43 Abs. 2 des Telekommunikationsgesetzes festgelegten Bedingungen und Regelungen und der dem Netzbetreiber aufgegebenen Verpflichtungen. Dies gilt auch für Kunden, deren Anbieter nicht zugleich Netzbetreiber sind. Mit der Zuteilung der Teilnehmerrufnummer erwirbt der Endkunde im Rahmen des Telekommunikationsgesetzes und der Bedingungen und Regelungen nach § 43 Abs. 2 des Telekommunikationsgesetzes ein vom Anbieter unabhängiges dauerhaftes Nutzungsrecht an der Teilnehmerrufnummer. Die Teilnehmerrufnummer ist rechtsgeschäftlich nicht übertragbar.

(3) Kunden müssen Änderungen von Teilnehmerrufnummern hinnehmen, wenn diese durch Maßnahmen oder Entscheidungen der Regulierungsbehörde gegenüber dem Anbieter nach § 43 des Telekommunikationsgesetzes und der dazu ergangenen Verfahrensregelungen veranlasst sind oder die Zuteilung auf Grund unrichtiger Angaben des Kunden erfolgt ist.

(4) Für die Zuteilung der Teilnehmerrufnummer kann der Anbieter nur die mit der Zuteilung verbundenen Kosten verlangen.

(5) Teilnehmerrufnummern, die bis zum Zeitpunkt des Inkrafttretens dieser Verordnung vom Anbieter vergeben wurden, gelten als zugeteilt.

(6) Einwendungen gegen die Rufnummernzuteilung oder gegen Änderungen der Teilnehmerrufnummern kann der Kunde seinem Anbieter gegenüber nur innerhalb einer Ausschlussfrist von sechs Wochen ab Zugang der schriftlichen Zuteilung geltend machen. War der Kunde ohne Verschulden verhindert, diese Einwendungsfrist einzuhalten, so kann er die Einwendungen innerhalb von zwei Wochen nach Wegfall des Hindernisses nachholen. Der Kunde ist in der schriftlichen Zuteilung auf die Frist hinzuweisen.

§ 21
Aufnahme in öffentliche Teilnehmerverzeichnisse

(1) Der Kunde kann von seinem Anbieter von Sprachkommunikationsdienstleistungen für die Öffentlichkeit verlangen, in ein allgemein zugängliches, nicht notwendig anbietereigenes Teilnehmerverzeichnis unentgeltlich eingetragen zu werden, seinen Eintrag prüfen und berichtigen oder wieder streichen lassen.

(2) Die Teilnehmerverzeichnisse enthalten mindestens die Rufnummer, den Namen, den Vornamen und die Anschrift des Inhabers des Netzzugangs, soweit sie dem Anbieter zugänglich sind und in Kundenverzeichnissen veröffentlicht werden dürfen. Der Inhaber des Netzzugangs kann im Rahmen der datenschutzrechtlichen Bestimmungen verlangen, dass Mitbenutzer entgeltlich eingetragen werden. Der Anspruch steht auch Wiederverkäufern von Sprachkommunikationsdienstleistungen für deren Kunden zu. Die Vorschriften über das Recht des Kunden, der Eintragung seiner Daten in Teilnehmerverzeichnisse ganz oder teilweise zu widersprechen, bleiben unberührt.

(3) Die Anbieter tragen dafür Sorge, dass die Eintragungen in das Verzeichnis für alle Teilnehmer in nichtdiskriminierender Weise erfolgen.

(4) Ein Unternehmen, das nach § 19 des Telekommunikationsgesetzes zur Herausgabe von Teilnehmerverzeichnissen verpflichtet wurde oder das diese Leistung nach § 97 Abs. 1 des Telekommunikationsgesetzes erbringt, kann die Teilnehmerdaten von den Anbietern von Sprachkommunikationsdienstleistungen für die Öffentlichkeit verlangen. Ein hierfür erhobenes Entgelt hat sich an den Kosten der effizienten Leistungsbereitstellung zu orientieren.

(5) Die Absätze 1 bis 4 gelten entsprechend für die Aufnahme in Verzeichnisse für Auskunftsdienste.

§ 22
Überlassung von Teilnehmerverzeichnissen

Der Kunde kann von seinem Anbieter von Sprachkommunikationsdienstleistungen für die Öffentlichkeit die in der Regel jährliche Überlassung eines Teilnehmerverzeichnisses mit den Rufnummern des regionalen Teilnehmerbereichs verlangen.
X

X
X
Vierter Teil
Kundeninformationen

§ 27
Veröffentlichung von Kundeninformationen

(1) Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit haben allgemeine Informationen für Endkunden zu veröffentlichen und in einer für alle Interessierten leicht zugänglichen Weise bereitzustellen. Hierzu zählen Informationen über Zugang, Nutzungs- und Lieferbedingungen, das Recht des Kunden, der Eintragung seiner Daten in Teilnehmerverzeichnisse ganz oder teilweise zu widersprechen sowie Entgelte sowie beim Angebot von Sprachtelefondienst Angaben über die Qualitätskennwerte nach § 32. Satz 1 ist erfüllt, wenn diese Angaben im Amtsblatt der Regulierungsbehörde veröffentlicht werden und in den

Geschäftsstellen der Anbieter für den Kunden bereitgehalten werden. Erfolgt die Veröffentlichung der Kundeninformationen an anderer Stelle, hat der Anbieter die Fundstelle umgehend der Regulierungsbehörde mitzuteilen. Die Regulierungsbehörde veröffentlicht einen Hinweis auf die Fundstelle in ihrem Amtsblatt.

(2) Anbieter von Zugängen zu festen öffentlichen Telekommunikationsnetzen haben über die Verpflichtung nach Absatz 1 hinaus die technischen Merkmale der Schnittstellen nach Maßgabe des Anhangs zu § 27 Abs. 2 entsprechend Absatz 1 zu veröffentlichen. Änderungen bestehender oder Einführung neuer Schnittstellenspezifikationen sind drei Monate vor ihrer Einführung zu veröffentlichen.

(3) Marktbeherrschende Anbieter von Übertragungswegen haben über die Verpflichtung nach Absatz 1 hinaus Informationen über technische Merkmale, üblicherweise erreichte Qualitätsmerkmale, sowie die Bedingungen für die Anschließung von Endeinrichtungen in einer mit Artikel 4 und Anhang I der Richtlinie 92/44/EWG des Rates vom 5. Juni 1992 zur Einführung des offenen Netzzugangs bei Mietleitungen (ABl. EG Nr. L 165 S. 27) in der Fassung der Richtlinie 97/51/EG des Europäischen Parlaments und des Rates vom 6. Oktober 1997 zur Anpassung der Richtlinien 90/387/EWG und 92/44/EWG an ein wettbewerbsorientiertes Telekommunikationsumfeld (ABl. EG Nr. L 295, S. 23) übereinstimmenden Form entsprechend Absatz 1 zu veröffentlichen.

(4) Die allgemeinen Informationen für Endkunden über allgemeine Zugänge zu festen öffentlichen Telekommunikationsnetzen müssen Angaben über die Regelbereitstellungsfrist, die Regelentstörfrist, Ausgleichsregelungen bei Leistungsstörungen sowie eine Zusammenfassung des Vorgehens zur Einleitung von Schlichtungsverfahren nach § 35 enthalten. Auf die Möglichkeit einer Benachrichtigung nach § 6 Abs. 3 ist hinzuweisen.

§ 28
Allgemeine Geschäftsbedingungen; Vertragsänderungen

(1) Soweit Allgemeine Geschäftsbedingungen der Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit nach § 23 Abs. 2 Nr. 1a des AGB-Gesetzes in die Verträge einbezogen werden, weist der Anbieter in seinen Auftragsformblättern auf die Tatsache der Veröffentlichung im Amtsblatt der Regulierungsbehörde und die Möglichkeit der Einsichtnahme bei seinen Geschäftsstellen hin.

(2) Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit können bestehende Verträge durch Einbeziehung Allgemeiner Geschäftsbedingungen, Leistungsbeschreibungen und Entgelte entsprechend § 23 Abs. 2 Nr. 1a des AGB-Gesetzes ändern. § 27 findet Anwendung.

(3) Über Vertragsänderungen, die nach Absatz 2 erfolgen, und deren Inhalte sind die Kunden in geeigneter Weise und unter Hinweis auf die Fundstelle der Veröffentlichung zu informieren. Werden Verträge nach Absatz 2 zuungunsten der Kunden geändert, so kann der betroffene Kunde das Vertragsverhältnis für den Zeitpunkt des Wirksamwerdens der Änderung kündigen. Der Kunde ist auf das Kündigungsrecht hinzuweisen. Änderungen zuungunsten der Kunden werden vor dieser Information nicht wirksam. Das Kündigungsrecht erlischt, wenn der Kunde nicht innerhalb eines Monats nach der Information davon Gebrauch macht.

(4) Rückwirkende Vertragsänderungen sind unbeschadet des § 29 Abs. 2 des Telekommunikationsgesetzes nur zugunsten des Kunden und ausschließlich zum Zwecke nachträglicher Beseitigung eingetretener Wettbewerbsstörungen unter Beachtung des Diskriminierungsverbotes zulässig. § 1 Abs. 2 findet keine Anwendung.

§ 29
Veröffentlichungsfristen

(1) Änderungen von Entgelten und entgeltrelevanten Bestandteilen Allgemeiner Geschäftsbedingungen marktbeherrschender Anbieter von Sprachtelefondienst und von Übertragungswegen treten frühestens einen Monat nach ihrer Veröffentlichung in Kraft. Die Frist gilt nicht für kurzzeitige ereignisbezogene Sondertarife. Informationen über neue Angebote marktbeherrschender Anbieter von Übertragungswegen sind so bald wie möglich zu veröffentlichen. Die Regulierungsbehörde kann eine Abweichung von der Frist nach Satz 1 in Einzelfällen genehmigen.

(2) Bei genehmigungspflichtigen Entgelten und entgeltrelevanten Bestandteilen Allgemeiner Geschäftsbedingungen darf die Veröffentlichung nach Absatz 1 nicht vor Erteilung der Genehmigung erfolgen.

§ 30
Vereinbarung von Leistungen ohne Entgeltgenehmigung

Wird ein genehmigungspflichtiges Entgelt vereinbart, für das eine Genehmigung nach dem Gesetz oder eine vorläufige Anordnung der Regulierungsbehörde nicht vorliegt, und existiert auch kein Entgelt, das nach § 29 Abs. 2 Satz 1 des Telekommunikationsgesetzes an die Stelle des vereinbarten Entgeltes tritt, so ist die Vereinbarung unwirksam.

§ 31
Abschaltung von Endeinrichtungen

Werden Endeinrichtungen eines Kunden nach § 59 Absatz 6 Satz 1 des Telekommunikationsgesetzes abgeschaltet, so hat der Anbieter des Netzzugangs den Kunden unverzüglich unter Angabe der Gründe und unter Hinweis auf sein Widerspruchsrecht nach § 59 Absatz 6 Satz 2 des Telekommunikationsgesetzes über die Abschaltung zu unterrichten. Sobald die beanstandete Endeinrichtung von der Abschlusseinrichtung getrennt worden ist, ist der Zugang wieder bereitzustellen.
X

X
X

Fünfter Teil
Verfahren der Regulierungsbehörde

§ 34
Verfahren bei Zugangsbeschränkung

(1) Schränkt ein marktbeherrschender Anbieter von Übertragungswegen die Bereitstellung oder Verfügbarkeit eines Übertragungsweges ein, so kann der betroffene Kunde die Regulierungsbehörde zur Entscheidung über die Berechtigung der Zugangsbeschränkung nach den Vorschriften des Telekommunikationsgesetzes und der aufgrund des Telekommunikationsgesetzes erlassenen Verordnungen anrufen. Die begründete Entscheidung der Regulierungsbehörde ist den Parteien innerhalb einer Woche nach Beschlussfassung bekannt zu geben.

(2) Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit können bei Sperrung, Beendigung, wesentlicher Änderung oder Einschränkung der Verfügbarkeit von Diensten, die ihnen von marktbeherrschenden Anbietern von Sprachtelefondienstleistungen bereitgestellt werden, die Regulierungsbehörde zur

Entscheidung über die Berechtigung der Beschränkung nach den Vorschriften des Telekommunikationsgesetzes und der aufgrund des Telekommunikationsgesetzes erlassenen Verordnungen anrufen. Absatz 1 Satz 2 findet Anwendung.

(3) Die Regulierungsbehörde veröffentlicht einmal jährlich eine Übersicht über die Verfahren nach Absatz 1 und 2 in ihrem Amtsblatt.

§ 35
Schlichtung

(1) Macht der Endkunde eines Anbieters von Zugängen zu einem öffentlichen Telekommunikationsnetz oder eines Sprachtelefondienstanbieters die Verletzung eigener Rechte geltend, die ihm aufgrund dieser Verordnung zustehen, kann er die Regulierungsbehörde zum Zwecke der Streitbeilegung anrufen.

(2) Die Regulierungsbehörde hört die Beteiligten mit dem Ziel einer gütlichen Einigung an. Das Verfahren endet mit einer Einigung der Parteien oder der Feststellung der Regulierungsbehörde, dass eine Einigung der Parteien nicht zustande gekommen ist. Dieses Ergebnis ist den Parteien schriftlich mitzuteilen.

(3) Jede Partei trägt die ihr durch die Teilnahme am Verfahren entstandenen Kosten selbst.

(4) Das Verfahren nach den Absätzen 1 bis 3 steht auch Kunden marktbeherrschender Anbieter von Übertragungswegen offen.

§ 36
Sicherstellung des Universaldienstes

Marktbeherrschende Anbieter von Sprachtelefondienst, die einen Vertragsabschluss über die Inanspruchnahme von Sprachtelefondienst oder damit in unmittelbarem Zusammenhang stehender Universaldienstleistungen ablehnen, ohne dass der Kunde auf die Leistungen verzichtet, haben dies unter Angabe der Gründe umgehend der Regulierungsbehörde anzuzeigen. Die Regulierungsbehörde trägt im Rahmen des Verfahrens zur Sicherstellung von Universaldienstleistungen dafür Sorge, dass dem Kunden die Leistungen bereitgestellt werden.

III.1 Teledienstegesetz - TDG

Abschnitt 1
Allgemeine Bestimmungen

§ 1
Zweck des Gesetzes

Zweck des Gesetzes ist es, einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen.

§ 2
Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).

(2) Teledienste im Sinne von Absatz 1 sind insbesondere

1. Angebote im Bereich der Individualkommunikation (z.B. Telebanking, Datenaustausch),

2. Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, zum Beispiel Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote),

3. Angebote zur Nutzung des Internets oder weiterer Netze,

4. Angebote zur Nutzung von Telespielen,

5. Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit

(3) Absatz 1 gilt unabhängig davon, ob die Nutzung der Teledienste ganz oder teilweise unentgeltlich oder gegen Entgelt möglich ist.

(4) Dieses Gesetz gilt nicht für

1. Telekommunikationsdienstleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten nach § 3 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120),

2. Rundfunk im Sinne des § 2 des Rundfunkstaatsvertrages,

3. inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach § 2 des Mediendienste-Staatsvertrages in der Fassung vom 20. Januar bis 7. Februar 1997,

4. den Bereich der Besteuerung.

(5) Presserechtliche Vorschriften bleiben unberührt.

(6) Dieses Gesetz schafft weder Regelungen im Bereich des internationalen Privatrechts noch befasst es sich mit der Zuständigkeit der Gerichte.

§ 3
Begriffsbestimmungen

Im Sinne dieses Gesetzes bezeichnet der Ausdruck

1. „Diensteanbieter“ jede natürliche oder juristische Person, die eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt;

2. „Nutzer“ jede natürliche oder juristische Person, die zu beruflichen oder sonstigen Zwecken Teledienste in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen;

3. „Verteildienste“ Teledienste, die im Wege einer Übertragung von Daten ohne individuelle Anforderung gleichzeitig für eine unbegrenzte Zahl von Nutzern erbracht werden;

4. „Abrufdienste“ Teledienste, die im Wege einer Übertragung von Daten auf Anforderung eines einzelnen Nutzers erbracht werden;

5. „kommerzielle Kommunikation“ jede Form der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren, Dienstleistungen oder des Erscheinungsbilds eines Unternehmens, einer sonstigen Organisation oder einer natürlichen Person dient, die eine Tätigkeit im Handel, Gewerbe oder Handwerk oder einen freien Beruf ausübt; die folgenden Angaben stellen als solche keine Form der kommerziellen Kommunikation dar:

   a) Angaben, die direkten Zugang zur Tätigkeit des Unternehmens oder der Organisation oder Person ermöglichen, wie insbesondere ein Domain-Name oder eine Adresse der elektronischen Post;

   b) Angaben in bezug auf Waren und Dienstleistungen oder das Erscheinungsbild eines Unternehmens, einer Organisation oder Person, die unabhängig und insbesondere ohne finanzielle Gegenleistung gemacht werden;

6. „niedergelassener Diensteanbieter“ Anbieter, die mittels einer festen Einrichtung auf unbestimmte Zeit Teledienste geschäftsmäßig anbieten oder erbringen; der Standort der technischen Einrichtung allein begründet keine Niederlassung des Anbieters.

Einer juristischen Person steht eine Personengesellschaft gleich, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben und Verbindlichkeiten einzugehen.

§ 4
Herkunftslandprinzip

(1) In der Bundesrepublik Deutschland niedergelassene Diensteanbieter und ihre Teledienste unterliegen den Anforderungen des deutschen Rechts auch dann, wenn die Teledienste in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (ABl. EG Nr. L 178 S. 1) geschäftsmäßig angeboten oder erbracht werden.

(2) Der freie Dienstleistungsverkehr von Telediensten, die in der Bundesrepublik Deutschland von Diensteanbietern geschäftsmäßig angeboten oder erbracht werden, die in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinie 2000/31/EG niedergelassen sind, wird nicht eingeschränkt. Absatz 5 bleibt unberührt.

(3) Von den Absätzen 1 und 2 bleiben unberührt

1. die Freiheit der Rechtswahl,

2. die Vorschriften für vertragliche Schuldverhältnisse in bezug auf Verbraucherverträge,

3. gesetzliche Vorschriften über die Form des Erwerbs von Grundstücken und grundstücksgleichen Rechten sowie der Begründung, Übertragung, Änderung oder Aufhebung von dinglichen Rechten an Grundstücken und grundstücksgleichen Rechten.

(4) Die Absätze 1 und 2 gelten nicht für

1. die Tätigkeit von Notaren sowie von Angehörigen anderer Berufe, soweit diese ebenfalls hoheitlich tätig sind,

2. die Vertretung von Mandanten und die Wahrnehmung ihrer Interessen vor Gericht,

3. die Zulässigkeit nicht angeforderter kommerzieller Kommunikationen durch elektronische Post,

4. Gewinnspiele mit einem einen Geldwert darstellenden Einsatz bei Glücksspielen, einschließlich Lotterien und Wetten,

5. die Anforderungen an Verteildienste,

6. das Urheberrecht, verwandte Schutzrechte, Rechte im Sinne der Richtlinie 87/54/EWG des Rates vom 16. Dezember 1986 über den Rechtsschutz der Topographien von Halbleitererzeugnissen (ABl. EG Nr. L 24 S. 36) und der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken (ABl. EG Nr. L 77 S. 20) sowie für gewerbliche Schutzrechte,

7. die Ausgabe elektronischen Geldes durch Institute, die gemäß Artikel 8 Abs. 1 der Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (ABL. EG Nr. L 275 S. 39) von der Anwendung einiger oder aller Vorschriften dieser Richtlinie und von der Anwendung der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates vom 20. März 2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (ABl. EG Nr. L 126 S. 1) freigestellt sind,

8. Vereinbarungen oder Verhaltensweisen, die dem Kartellrecht unterliegen,

9. die von den §§ 12, 13a bis 13c, 55a, 83, 110a bis 110d, 111b und 111c des Versicherungsaufsichtsgesetzes und der Verordnung über die Berichterstattung von Versicherungsunternehmen gegenüber dem Bundesaufsichtsamt für das Versicherungswesen erfassten Bereiche, die Regelungen über das auf Versicherungsverträge anwendbare Recht sowie für Pflichtversicherungen,

10. das für den Schutz personenbezogener Daten geltende Recht.

(5) Das Angebot und die Erbringung eines Teledienstes durch einen Diensteanbieter, der in einem anderen Staat im Geltungsbereich der Richtlinie 2000/31/EG niedergelassen ist, unterliegen abweichend von Absatz 2 den Einschränkungen des innerstaatlichen Rechts, soweit dieses dem Schutz

1. der öffentlichen Ordnung, insbesondere im Hinblick auf die Verhütung, Ermittlung, Aufklärung, Verfolgung und Vollstreckung von Straftaten und Ordnungswidrigkeiten, einschließlich des Jugendschutzes und der

Bekämpfung der Hetze aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität sowie von Verletzungen der Menschenwürde einzelner Personen,

2. der öffentlichen Sicherheit, insbesondere der Wahrung nationaler Sicherheits- und Verteidigungsinteressen,

3. der öffentlichen Gesundheit,

4. der Interessen der Verbraucher, einschließlich des Schutzes von Anlegern, vor Beeinträchtigungen oder ernsthaften und schwerwiegenden Gefahren dient, und die auf der Grundlage des innerstaatlichen Rechts in Betracht kommenden Maßnahmen in einem angemessenen Verhältnis zu diesen Schutzzielen stehen. Für das Verfahren zur Einleitung von Maßnahmen nach Satz 1 – mit Ausnahme von gerichtlichen Verfahren einschließlich etwaiger Vorverfahren und der Verfolgung von Straftaten einschließlich der Strafvollstreckung und von Ordnungswidrigkeiten – sieht Artikel 3 Abs. 4 und 5 der Richtlinie 2000/31/EG Konsultations- und Informationspflichten vor.

Abschnitt 2.
Zugangsfreiheit und Informationspflichten

§ 5
Zugangsfreiheit

Teledienste sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

§ 6
Allgemeine Informationspflichten

Diensteanbieter haben für geschäftsmäßige Teledienste mindestens folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich den Vertretungsberechtigten,

2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,

3. soweit der Teledienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,

4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,

5. soweit der Teledienst in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens 3-jährige Berufsausbildung abschließen (ABl. EG Nr. L 19 S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung beruflicher Befähigungsnachweise in Ergänzung zur Richtlinie 89/48/EWG (Abl. EG Nr. L 209 S. 25), die zuletzt durch die Richtlinie 97/38/EG der Kommission vom 20. Juni 1997 (ABl. EG Nr. 184 S. 31) geändert worden ist, angeboten oder erbracht wird, Angaben über

   a) die Kammer, welcher die Diensteanbieter angehören,

b) die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,

c) die Bezeichnung der berufsrechtlichen Regelungen und dazu, wie diese zugänglich sind,

6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes besitzen, die Angabe dieser Nummer.

Weitergehende Informationspflichten, insbesondere nach dem Fernabsatzgesetz, dem Fernunterrichtsschutzgesetz, dem Teilzeit-Wohnrechtegesetz oder dem Preisangaben- und Preisklauselgesetz und der Preisangabenverordnung, dem Versicherungsaufsichtsgesetz sowie nach handelsrechtlichen Bestimmungen bleiben unberührt.

§ 7
Besondere Informationspflichten bei kommerziellen Kommunikationen

Diensteanbieter haben bei kommerziellen Kommunikationen, die Bestandteil eines Teledienstes sind oder die einen solchen Dienst darstellen, mindestens die nachfolgenden Voraussetzungen zu beachten:

1. Kommerzielle Kommunikationen müssen klar als solche zu erkennen sein.

2. Die natürliche oder juristische Person, in deren Auftrag kommerzielle Kommunikationen erfolgen, muss klar identifizierbar sein.

3. Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke müssen klar als solche erkennbar sein, und die Bedingungen für ihre Inanspruchnahme müssen leicht zugänglich sein sowie klar und unzweideutig angegeben werden.

4. Preisausschreiben oder Gewinnspiele mit Werbecharakter müssen klar als solche erkennbar und die Teilnahmebedingungen leicht zugänglich sein sowie klar und unzweideutig angegeben werden.

Die Vorschriften des Gesetzes gegen den unlauteren Wettbewerb bleiben unberührt.

Abschnitt 3
Verantwortlichkeit

§ 8
Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter im Sinne der §§ 9 bis 11 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des

Diensteanbieters nach den §§ 9 bis 11 unberührt. Das Fernmeldegeheimnis nach § 85 des Telekommunikationsgesetzes ist zu wahren.

§ 9
Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

1. die Übermittlung nicht veranlasst,

2. den Adressaten der übermittelten Informationen nicht ausgewählt und

3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

§ 10
Zwischenspeicherung zur beschleunigten Übermittlung von Informationen

Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung der fremden Information an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie

1. die Informationen nicht verändern,

2. die Bedingungen für den Zugang zu den Informationen beachten,

3. die Regeln für die Aktualisierung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,

4. die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und

5. unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

§ 9 Abs. 1 Satz 2 gilt entsprechend.

§ 11

Speicherung von Informationen

Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern

1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder

2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.

Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Abschnitt 4
Bußgeldvorschriften

§ 12

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 6 Satz 1 eine Information nicht, nicht richtig oder nicht vollständig verfügbar hält.

(2) die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

III.2 Teledienstedatenschutzgesetz (TDDSG)

§ 1
Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für den Schutz personenbezogener Daten der Nutzer von Telediensten im Sinne des Teledienstegesetzes bei der Erhebung, Verarbeitung und Nutzung dieser Daten durch Diensteanbieter. Sie gelten nicht bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten

1. im Dienst- und Arbeitsverhältnis, soweit die Nutzung der Teledienste zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt,

2. innerhalb von oder zwischen Unternehmen oder öffentlichen Stellen, soweit die Nutzung der Teledienste zur ausschließlichen Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

(2) Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden.

§ 2
Begriffsbestimmungen

Im Sinne dieses Gesetzes bezeichnet der Ausdruck

1. „Diensteanbieter“ jede natürliche oder juristische Person, die eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt,

2. „Nutzer“ jede natürliche Person, die Teledienste in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

Einer juristischen Person steht eine Personengesellschaft gleich, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben und Verbindlichkeiten einzugehen.

§ 3

Grundsätze

(1) Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Durchführung von Telediensten erhobene personenbezogene Daten für andere Zwecke nur verarbeiten und nutzen, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(3) Die Einwilligung kann unter den Voraussetzungen von § 4 Abs. 2 elektronisch erklärt werden.

(4) Der Diensteanbieter darf die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in nicht zumutbarer Weise möglich ist.

§ 4
Pflichten des Diensteanbieters

(1) Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

(2) Bietet der Diensteanbieter dem Nutzer die elektronische Einwilligung an, so hat er sicherzustellen, dass

1. sie nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen kann,

2. die Einwilligung protokolliert wird und

3. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann.

(3) Der Diensteanbieter hat den Nutzer vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Absatz 1 Satz 3 gilt entsprechend.

(4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. der Nutzer seine Verbindung mit dem Diensteanbieter jederzeit abbrechen kann,

2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder gesperrt werden können,

3. der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,

4. die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden können,

5. Daten nach § 6 Abs. 2 nur für Abrechnungszwecke und

6. Nutzerprofile nach § 6 Abs. 3 nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden können.

An die Stelle der Löschung nach Nummer 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

(5) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(6) Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

(7) Der Diensteanbieter hat dem Nutzer auf Verlangen unentgeltlich und unverzüglich Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.

§ 5
Bestandsdaten

Der Diensteanbieter darf personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten und nutzen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich sind (Bestandsdaten). Nach Maßgabe der hierfür geltenden Bestimmungen darf der Diensteanbieter Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung erteilen.

§ 6
Nutzungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

a) Merkmale zur Identifikation des Nutzers,

b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und

c) Angaben über die vom Nutzer in Anspruch genommenen Teledienste.

(2) Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Teledienste zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.

(3) Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 4 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren.

(5) Der Diensteanbieter darf an andere Diensteanbieter oder Dritte Abrechnungsdaten übermitteln, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer erforderlich ist. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Handelt es sich dabei um Daten, die beim Diensteanbieter auch dem Fernmeldegeheimnis unterliegen, ist der Dritte zur Wahrung des Fernmeldegeheimnisses zu verpflichten. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen anonymisierte Nutzungsdaten übermittelt werden. Nach Maßgabe der hierfür geltenden Bestimmungen darf der Diensteanbieter Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung erteilen.

(6) Die Abrechnung über die Inanspruchnahme von Telediensten darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Teledienste nicht erkennen lassen, es sei denn, der Nutzer verlangt einen Einzelnachweis.

(7) Der Diensteanbieter darf Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers verarbeitet werden, höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung speichern. Werden gegen die Entgeltforderung innerhalb dieser Frist Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen, dürfen die Abrechnungsdaten aufbewahrt werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen ist.

(8) Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus nur verarbeiten und nutzen, soweit dies zur Durchsetzung seiner Ansprüche gegenüber dem Nutzer erforderlich ist. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.

§ 7
Auskunftsrecht des Nutzers

(aufgehoben)

§ 8
Bundesbeauftragter für den Datenschutz

Der Bundesbeauftragte für den Datenschutz beobachtet die Entwicklung des Datenschutzes bei Telediensten und nimmt dazu im Rahmen seines Tätigkeitsberichtes nach § 26 Abs. 1 Bundesdatenschutzgesetz Stellung.

§ 9
Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 3 Abs. 4 die Erbringung von Telediensten von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig macht,

2. entgegen § 4 Abs. 1 Satz 1 oder Satz 2 den Nutzer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

3. entgegen § 4 Abs. 2 oder 4 Satz 1 Nr. 1 bis 5 einer dort genannten Pflicht zur Sicherstellung nicht oder nicht richtig nachkommt,

4. entgegen § 5 Satz 1 oder § 6 Abs. 1 Satz 1 oder Abs. 8 Satz 1 oder 2 personenbezogene Daten erhebt, verarbeitet, nutzt oder nicht oder nicht rechtzeitig löscht oder

5. entgegen § 6 Abs. 3 Satz 3 ein Nutzungsprofil mit Daten über den Träger des Pseudonyms zusammenführt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

IV.1 Auszug aus dem Strafgesetzbuch (StGB)

§ 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.

§ 203
Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist.

4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,

2. für den öffentlichen Dienst besonders Verpflichteten,

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,

5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(3) Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlass erlangt hat.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 205
Strafantrag

(1) In den Fällen des § 201 Abs. 1 und 2 und der §§ 202 bis 204 wird die Tat nur auf Antrag verfolgt.

(2) Stirbt der Verletzte, so geht das Antragsrecht nach § 77 Abs. 2 auf die Angehörigen über; dies gilt nicht in den Fällen des § 202a. Gehört das Geheimnis nicht zum persönlichen Lebensbereich des Verletzten, so geht das Antragsrecht bei Straftaten nach den §§ 203 und 204 auf die Erben über. Offenbart oder verwertet der Täter in den Fällen der §§ 203 und 204 das Geheimnis nach dem Tod des Betroffenen, so gelten die Sätze 1 und 2 sinngemäß.

§ 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.

IV.2 Auszug aus der Strafprozessordnung (StPO)

§ 100a

Die Überwachung und Aufzeichnung der Telekommunikation darf angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer

1. a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates oder des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 80 bis 82, 84 bis 86, 87 bis 89, 94 bis 100a des Strafgesetzbuches, § 20 Abs. 1 Nr. 1 bis 4 des Vereinsgesetzes),

   b) Straftaten gegen die Landesverteidigung (§§ 109d bis 109h des Strafgesetzbuches),

   c) Straftaten gegen die öffentliche Ordnung (§§ 129 bis 130 des Strafgesetzbuches, § 92 Abs. 1 Nr. 7 des Ausländergesetzes),

   d) ohne Soldat zu sein, Anstiftung oder Beihilfe zur Fahnenflucht oder Anstiftung zum Ungehorsam (§§ 16, 19 in Verbindung mit § 1 Abs. 3 des Wehrstrafgesetzes),

   e) Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages oder der im Land Berlin anwesenden Truppen einer der Drei Mächte (§§ 89, 94 bis 97, 98 bis 100, 109d bis 109g des Strafgesetzbuches, §§ 16, 19 des Wehrstrafgesetzes in Verbindung mit Artikel 7 des Vierten Strafrechtsänderungsgesetzes),

2. eine Geld- oder Wertpapierfälschung (§§ 146, 151, 152 des Strafgesetzbuches),
   einen schweren Menschenhandel nach § 181 Abs. 1 Nr. 2, 3 des Strafgesetzbuches,
   einen Mord, einen Totschlag oder einen Völkermord (§§ 211, 212, 220a des Strafgesetzbuches),
   eine Straftat gegen die persönliche Freiheit (§§ 234, 234a, 239a, 239b des Strafgesetzbuches),
   einen Bandendiebstahl (§ 244 Abs. 1 Nr. 2 des Strafgesetzbuches) oder einen schweren Bandendiebstahl (§ 244a des Strafgesetzbuches),

einen Raub oder eine räuberische Erpressung (§§ 249 bis 251, 255 des Strafgesetzbuches),
eine Erpressung (§ 253 des Strafgesetzbuches),
eine gewerbsmäßige Hehlerei, eine Bandenhehlerei (§ 260 des Strafgesetzbuches) oder eine gewerbsmäßige Bandenhehlerei (§ 260a des Strafgesetzbuches),
eine Geldwäsche, eine Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 oder 4 des Strafgesetzbuches,
eine gemeingefährliche Straftat in den Fällen der §§ 306 bis 306c oder 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314 oder 315 Abs. 3, des § 315b Abs. 3 oder der §§ 316a oder 316c des Strafgesetzbuches,

3. eine Straftat nach § 52a Abs. 1 bis 3, § 53 Abs. 1 Satz 1 Nr. 1, 2, Satz 2 des Waffengesetzes, § 34 Abs. 1 bis 6 des Außenwirtschaftsgesetzes oder nach § 19 Abs. 1 bis 3 § 20 Abs. 1 oder 2, jeweils auch in Verbindung mit § 21, oder § 22a Abs. 1 bis 3 des Gesetzes über die Kontrolle von Kriegswaffen,

4. eine Straftat nach einer in § 29 Abs. 3 Satz 2 Nr. 1 des Betäubungsmittelgesetzes in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen oder eine Straftat nach §§ 29a, 30 Abs. 1 Nr. 1, 2, 4, § 30a oder § 30b des Betäubungsmittelgesetzes oder

5. eine Straftat nach § 92a Abs. 2 oder § 92b des Ausländergesetzes oder nach § 84 Abs. 3 oder § 84a des Asylverfahrensgesetzes

begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, und wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

§ 100b

(1) Die Überwachung und Aufzeichnung der Telekommunikation (§ 100a) darf nur durch den Richter angeordnet werden. Bei Gefahr im Verzug kann die Anordnung

auch von der Staatsanwaltschaft getroffen werden. Die Anordnung der Staatsanwaltschaft tritt außer Kraft, wenn sie nicht binnen drei Tagen von dem Richter bestätigt wird.

(2) Die Anordnung ergeht schriftlich. Sie muss Namen und Anschrift des Betroffenen, gegen den sie sich richtet, und die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten. In ihr sind Art, Umfang und Dauer der Maßnahmen zu bestimmen. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die in § 100a bezeichneten Voraussetzungen fortbestehen.

(3) Auf Grund der Anordnung hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Hilfsbeamten (§ 152 des Gerichtsverfassungsgesetzes) die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, ergibt sich aus § 88 des Telekommunikationsgesetzes und der auf seiner Grundlage erlassenen Rechtsverordnung zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen. § 95 Abs. 2 gilt entsprechend.

(4) Liegen die Voraussetzungen des § 100a nicht mehr vor, so sind die sich aus der Anordnung ergebenden Maßnahmen unverzüglich zu beenden. Die Beendigung ist dem Richter und dem nach Absatz 3 Verpflichteten mitzuteilen.

(5) Die durch die Maßnahmen erlangten personenbezogenen Informationen dürfen in anderen Strafverfahren zu Beweiszwecken nur verwendet werden, soweit sich bei Gelegenheit der Auswertung Erkenntnisse ergeben, die zur Aufklärung einer der in § 100a bezeichneten Straftaten benötigt werden.

(6) Sind die durch die Maßnahmen erlangten Unterlagen zur Strafverfolgung nicht mehr erforderlich, so sind sie unverzüglich unter Aufsicht der Staatsanwaltschaft zu vernichten. Über die Vernichtung ist eine Niederschrift anzufertigen.

§ 100g

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von erheblicher Bedeutung, insbesondere eine der in § 100a

Satz 1 genannten Straftaten, oder mittels einer Endeinrichtung (§ 3 Nr. 3 des Telekommunikationsgesetzes) begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, darf angeordnet werden, dass diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, unverzüglich Auskunft über die in Absatz 3 bezeichneten Telekommunikationsverbindungsdaten zu erteilen haben, soweit die Auskunft für die Untersuchung erforderlich ist. Dies gilt nur, soweit diese Verbindungsdaten den Beschuldigten oder die sonstigen in § 100a Satz 2 bezeichneten Personen betreffen. Die Auskunft darf auch über zukünftige Telekommunikationsverbindungen angeordnet werden.

(2) Die Erteilung einer Auskunft darüber, ob von einem Telekommunikationsanschluss Telekommunikationsverbindungen zu den in Absatz 1 Satz 2 genannten Personen hergestellt worden sind, darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Telekommunikationsverbindungsdaten sind:

1. im Falle einer Verbindung Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung,

2. Beginn und Ende der Verbindung nach Datum und Uhrzeit,

3. vom Kunden in Anspruch genommene Telekommunikationsdienstleistung,

4. Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit.

§ 100h

(1) Die Anordnung muss den Namen und die Anschrift des Betroffenen, gegen den sie sich richtet, sowie die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten. Im Falle einer Straftat von erheblicher Bedeutung genügt eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, über die Auskunft erteilt werden soll, wenn andernfalls die Erforschung des Sachverhalts aussichtslos oder wesentlich erschwert wäre. § 100b Abs. 1, 2 Satz 1 und 3, Abs. 6 und § 95 Abs. 2 gelten entsprechend; im Falle der

Anordnung der Auskunft über zukünftige Telekommunikationsverbindungen gilt auch § 100b Abs. 2 Satz 4 und 5, Abs. 4 entsprechend.

(2) Soweit das Zeugnisverweigerungsrecht in den Fällen des § 53 Abs. 1 Nr. 1, 2 und 4 reicht, ist das Verlangen einer Auskunft über Telekommunikationsverbindungen, die von dem oder zu dem zur Verweigerung des Zeugnisses Berechtigten hergestellt wurden, unzulässig; eine dennoch erlangte Auskunft darf nicht verwertet werden. Dies gilt nicht, wenn die zur Verweigerung des Zeugnisses Berechtigten einer Teilnahme oder einer Begünstigung, Strafvereitelung oder Hehlerei verdächtig sind.

(3) Die durch die Auskunft erlangten personenbezogenen Informationen dürfen in anderen Strafverfahren zu Beweiszwecken nur verwendet werden, soweit sich bei Gelegenheit der Auswertung Erkenntnisse ergeben, die zur Aufklärung einer der in § 100g Abs. 1 Satz 1 bezeichneten Straftaten benötigt werden, oder wenn der Beschuldigte zustimmt.

§ 100i

(1) Durch technische Mittel dürfen
1. zur Vorbereitung einer Maßnahme nach § 100a die Geräte- und Kartennummer sowie
2. zur vorläufigen Festnahme nach § 127 Abs. 2 oder Ergreifung des Täters auf Grund eines Haftbefehls oder Unterbringungsbefehls der Standort eines aktiv geschalteten Mobilfunkendgerätes ermittelt werden.

(2) Die Maßnahme nach Absatz 1 Nr. 1 ist nur zulässig, wenn die Voraussetzungen des § 100a vorliegen und die Durchführung der Überwachungsmaßnahme ohne die Ermittlung der Geräte- oder Kartennummer nicht möglich oder wesentlich erschwert wäre. Die Maßnahme nach Absatz 1 Nr. 2 ist nur im Falle einer Straftat von erheblicher Bedeutung und nur dann zulässig, wenn die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder erschwert wäre; § 100c Abs. 2 Satz 2 gilt entsprechend. Die Maßnahme nach Absatz 1 Nr. 2 ist im Falle einer Straftat von erheblicher Bedeutung auch zulässig, wenn die Ermittlung des Aufenthaltsortes des Täters zur Eigensicherung der zur vorläufigen Festnahme oder Ergreifung eingesetzten Beamten des Polizeidienstes erforderlich ist.

(3) 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.

(4) § 100b Abs. 1 gilt entsprechend; im Falle der Anordnung zur Vorbereitung einer Maßnahme nach § 100a gilt auch § 100b Abs. 2 Satz 1 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 den Absätzen 1 und 2 bezeichneten Voraussetzungen fortbestehen. Auf Grund der Anordnung nach Absatz 1 Nr. 2 hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Hilfsbeamten (§ 152 des Gerichtsverfassungsgesetzes) die für die Ermittlung des Standortes des Mobilfunkendgerätes erforderliche Geräte- und Kartennummer mitzuteilen.

§ 101

(1) Von den getroffenen Maßnahmen (§§ 81e, 99, 100a, 100b, 100c Abs. 1 Nr. 1 Buchstabe b, Nr. 2 und 3, § 100d, 100g und 100h) sind die Beteiligten zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit, von Leib oder Leben einer Person sowie der Möglichkeit der weiteren Verwendung eines eingesetzten nicht offen ermittelnden Beamten geschehen kann. Erfolgt in den Fällen des § 100c Abs. 1 Nr. 3 die Benachrichtigung nicht binnen sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Benachrichtigung der richterlichen Zustimmung. Vor Erhebung der öffentlichen Klage entscheidet das in § 100d Abs. 2 Satz 1 genannte, danach das mit der Sache befasste Gericht.

(2) Sendungen, deren Öffnung nicht angeordnet worden ist, sind dem Beteiligten sofort auszuhändigen. Dasselbe gilt, soweit nach der Öffnung die Zurückbehaltung nicht erforderlich ist.

(3) Der Teil eines zurückbehaltenen Briefes, dessen Vorenthaltung nicht durch die Rücksicht auf die Untersuchung geboten erscheint, ist dem Empfangsberechtigten abschriftlich mitzuteilen.

(4) Entscheidungen und sonstige Unterlagen über Maßnahmen nach § 100c Abs. 1 Nr. 1 Buchstabe b, Nr. 2 und 3 werden bei der Staatsanwaltschaft verwahrt. Zu den

Akten sind sie erst zu nehmen, wenn die Voraussetzungen des Absatzes 1 erfüllt sind.

IV.3 Auszug aus dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10)

§ 1

Gegenstand des Gesetzes

(1) Es sind

1. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages,

2. der Bundesnachrichtendienst im Rahmen seiner Aufgaben nach § 1 Abs. 2 des BND-Gesetzes auch zu den in § 5 Abs. 1 Satz 3 Nr. 2 bis 6 und § 8 Abs. 1 Satz 1 bestimmten Zwecken

berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen, in den Fällen der Nummer 1 auch die dem Brief- oder Postgeheimnis unterliegenden Sendungen zu öffnen und einzusehen.

(2) Soweit Maßnahmen nach Absatz 1 von Behörden des Bundes durchgeführt werden, unterliegen sie der Kontrolle durch das Parlamentarische Kontrollgremium und durch eine besondere Kommission (G 10-Kommission).

§ 2

Pflichten der Anbieter von Post- und Telekommunikationsdiensten

(1) Wer geschäftsmäßig Postdienste erbringt oder an der Erbringung solcher Dienste mitwirkt, hat der berechtigten Stelle auf Anordnung Auskunft über die näheren Umstände des Postverkehrs zu erteilen und Sendungen, die ihm zum Einsammeln, Weiterleiten oder Ausliefern anvertraut sind, auszuhändigen. Der nach Satz 1 Verpflichtete hat der berechtigten Stelle auf Verlangen die zur Vorbereitung einer Anordnung erforderlichen Auskünfte zu Postfächern zu erteilen, ohne dass es hierzu einer gesonderten Anordnung bedarf. Wer geschäftsmäßig

Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt, hat der berechtigten Stelle auf Anordnung Auskunft über die näheren Umstände der nach Wirksamwerden der Anordnung durchgeführten Telekommunikation zu erteilen, Sendungen, die ihm zur Übermittlung auf dem Telekommunikationsweg anvertraut sind, auszuhändigen sowie die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. Ob und in welchem Umfang der nach Satz 3 Verpflichtete Vorkehrungen für die technische und organisatorische Umsetzung der Überwachungsmaßnahme zu treffen hat, bestimmt sich nach § 88 des Telekommunikationsgesetzes und der dazu erlassenen Rechtsverordnung.

(2) Der nach Absatz 1 Satz 1 oder 3 Verpflichtete hat vor Durchführung einer beabsichtigten Beschränkungsmaßnahme die Personen, die mit der Durchführung der Maßnahme betraut werden sollen,

1. einer einfachen Sicherheitsüberprüfung unterziehen zu lassen und

2. über Mitteilungsverbote nach § 17 sowie die Strafbarkeit eines Verstoßes nach § 18 zu belehren; die Belehrung ist aktenkundig zu machen.

Mit der Durchführung einer Beschränkungsmaßnahme dürfen nur Personen betraut werden, die nach Maßgabe des Satzes 1 überprüft und belehrt worden sind. Der nach Absatz 1 Satz 1 oder 3 Verpflichtete hat sicherzustellen, dass die Geheimschutzmaßnahmen nach den Abschnitten 1.1 bis 1.4, 1.6, 2.1 und 2.3 bis 2.5 der Anlage 7 zur Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen vom 29. April 1994 (GMBl. S. 674) getroffen werden.

(3) Die Sicherheitsüberprüfung nach Absatz 2 Satz 1 Nr. 1 ist entsprechend dem Sicherheitsüberprüfungsgesetz durchzuführen. Für Beschränkungsmaßnahmen einer Landesbehörde gilt dies nicht, soweit Rechtsvorschriften des Landes vergleichbare Bestimmungen enthalten; in diesem Fall sind die Rechtsvorschriften des Landes entsprechend anzuwenden. Zuständig ist bei Beschränkungsmaßnahmen von Bundesbehörden das Bundesministerium des Innern; im übrigen sind die nach Landesrecht bestimmten Behörden zuständig. Soll mit der Durchführung einer Beschränkungsmaßnahme eine Person betraut werden, für die innerhalb der letzten fünf Jahre bereits eine gleich- oder höherwertige Sicherheitsüberprüfung nach Bundes- oder Landesrecht durchgeführt worden ist, soll von einer erneuten Sicherheitsüberprüfung abgesehen werden.

§ 3
Voraussetzungen

(1) Beschränkungen nach § 1 Abs. 1 Nr. 1 dürfen unter den dort bezeichneten Voraussetzungen angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

1. Straftaten des Friedensverrats oder des Hochverrats (§§ 80 bis 83 des Strafgesetzbuches),

2. Straftaten der Gefährdung des demokratischen Rechtsstaates (§§ 84 bis 86, 87 bis 89 des Strafgesetzbuches, § 20 Abs. 1 Nr. 1 bis 4 des Vereinsgesetzes),

3. Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 94 bis 96, 97a bis 100a des Strafgesetzbuches),

4. Straftaten gegen die Landesverteidigung (§§ 109e bis 109g des Strafgesetzbuches),

5. Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages (§§ 87, 89, 94 bis 96, 98 bis 100, 109e bis 109g des Strafgesetzbuches in Verbindung mit Artikel 7 des Vierten Strafrechtsänderungsgesetzes vom 11. Juni 1957 (BGBl. I S. 597) in der Fassung des Gesetzes vom 25. Juni 1968 (BGBl. I S. 741),

6. Straftaten nach
   a) den §§ 129a und 130 des Strafgesetzbuches sowie
   b) den §§ 211, 212, 239a, 239b, 306 bis 306c, 308 Abs. 1 bis 3, § 315 Abs. 3, § 316b Abs. 3 und § 316c Abs. 1 und 3 des Strafgesetzbuches, soweit diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten, oder

7. Straftaten nach § 92 Abs. 1 Nr. 7 des Ausländergesetzes

plant, begeht oder begangen hat. Gleiches gilt, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind.

(2) Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Sie darf sich nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt. Maßnahmen, die sich auf Sendungen beziehen, sind nur hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen die Annahme rechtfertigen, dass sie von dem, gegen den sich die Anordnung richtet, herrühren oder für ihn bestimmt sind. Abgeordnetenpost von Mitgliedern des Deutschen Bundestages und der Parlamente der Länder darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet.

§ 4
Prüf-, Kennzeichnungs- und Löschungspflichten, Übermittlungen, Zweckbindung

(1) Die erhebende Stelle prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen ihrer Aufgaben allein oder zusammen mit bereits vorliegenden Daten für die in § 1 Abs. 1 Nr. 1 bestimmten Zwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. Sie unterbleibt, soweit die Daten für eine Mitteilung nach § 12 Abs. 1 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. In diesem Fall sind die Daten zu sperren; sie dürfen nur zu diesen Zwecken verwendet werden.

(2) Die verbleibenden Daten sind zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrecht zu erhalten. Die Daten dürfen nur zu den in § 1 Abs. 1 Nr. 1 und den in Absatz 4 genannten Zwecken verwendet werden.

(3) Der Behördenleiter oder sein Stellvertreter kann anordnen, dass bei der Übermittlung auf die Kennzeichnung verzichtet wird, wenn dies unerlässlich ist, um die Geheimhaltung einer Beschränkungsmaßnahme nicht zu gefährden, und die G 10-Kommission oder, soweit es sich um die Übermittlung durch eine Landesbehörde handelt, die nach Landesrecht zuständige Stelle zugestimmt hat. Bei Gefahr im Verzuge kann die Anordnung bereits vor der Zustimmung getroffen werden. Wird die

Zustimmung versagt, ist die Kennzeichnung durch den Übermittlungsempfänger unverzüglich nachzuholen; die übermittelnde Behörde hat ihn hiervon zu unterrichten.

(4) Die Daten dürfen nur übermittelt werden

1. zur Verhinderung oder Aufklärung von Straftaten, wenn
   a) tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 3 Abs. 1 genannten Straftaten plant oder begeht,
   b) bestimmte Tatsachen den Verdacht begründen, dass jemand eine sonstige in § 7 Abs. 4 Satz 1 genannte Straftat plant oder begeht,

2. zur Verfolgung von Straftaten, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Nummer 1 bezeichnete Straftat begeht oder begangen hat, oder

3. zur Vorbereitung und Durchführung eines Verfahrens nach Artikel 21 Abs. 2 Satz 2 des Grundgesetzes oder einer Maßnahme nach § 3 Abs. 1 Satz 1 des Vereinsgesetzes,

soweit sie zur Erfüllung der Aufgaben des Empfängers erforderlich sind.

(5) Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Verwendung dieser Daten ist unzulässig. Über die Übermittlung entscheidet ein Bediensteter der übermittelnden Stelle, der die Befähigung zum Richteramt hat. Die Übermittlung ist zu protokollieren.

(6) Der Empfänger darf die übermittelten Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind. Er prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die übermittelten Daten für diese Zwecke erforderlich sind. Absatz 1 Satz 2 und 3 gilt entsprechend. Der Empfänger unterrichtet die übermittelnde Stelle unverzüglich über die erfolgte Löschung.

X
X
X

§ 9

Antrag

(1) Beschränkungsmaßnahmen nach diesem Gesetz dürfen nur auf Antrag angeordnet werden.

(2) Antragsberechtigt sind im Rahmen ihres Geschäftsbereichs

1. das Bundesamt für Verfassungsschutz,
2. die Verfassungsschutzbehörden der Länder,
3. das Amt für den Militärischen Abschirmdienst und
4. der Bundesnachrichtendienst

durch den Behördenleiter oder seinen Stellvertreter.

(3) Der Antrag ist schriftlich zu stellen und zu begründen. Er muss alle für die Anordnung erforderlichen Angaben enthalten. In den Fällen der §§ 3 und 8 hat der Antragsteller darzulegen, dass die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

§ 10
Anordnung

(1) Zuständig für die Anordnung von Beschränkungsmaßnahmen ist bei Anträgen der Verfassungsschutzbehörden der Länder die zuständige oberste Landesbehörde, im Übrigen ein vom Bundeskanzler beauftragtes Bundesministerium.

(2) Die Anordnung ergeht schriftlich. In ihr sind der Grund der Anordnung und die zur Überwachung berechtigte Stelle anzugeben sowie Art, Umfang und Dauer der Beschränkungsmaßnahme zu bestimmen.

(3) In den Fällen des § 3 muss die Anordnung denjenigen bezeichnen, gegen den sich die Beschränkungsmaßnahme richtet. Bei einer Überwachung der Telekommunikation ist auch die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses anzugeben.

(4) In den Fällen der §§ 5 und 8 sind die Suchbegriffe in der Anordnung zu benennen. Ferner sind das Gebiet, über das Informationen gesammelt werden sollen, und die Übertragungswege, die der Beschränkung unterliegen, zu

bezeichnen. Weiterhin ist festzulegen, welcher Anteil der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität überwacht werden darf. In den Fällen des § 5 darf dieser Anteil höchstens zwanzig vom Hundert betragen.

(5) In den Fällen der §§ 3 und 5 ist die Anordnung auf höchstens drei Monate zu befristen. Verlängerungen um jeweils nicht mehr als drei weitere Monate sind auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

(6) Die Anordnung ist dem nach § 2 Abs. 1 Satz 1 oder 3 Verpflichteten insoweit mitzuteilen, als dies erforderlich ist, um ihm die Erfüllung seiner Verpflichtungen zu ermöglichen. Die Mitteilung entfällt, wenn die Anordnung ohne seine Mitwirkung ausgeführt werden kann.

(7) Das Bundesamt für Verfassungsschutz unterrichtet die jeweilige Landesbehörde für Verfassungsschutz über die in deren Bereich getroffenen Beschränkungsanordnungen. Die Landesbehörden für Verfassungsschutz teilen dem Bundesamt für Verfassungsschutz die in ihrem Bereich getroffenen Beschränkungsanordnungen mit.

§ 11
Durchführung

(1) Die aus der Anordnung sich ergebenden Beschränkungsmaßnahmen sind unter Verantwortung der Behörde, auf deren Antrag die Anordnung ergangen ist, und unter Aufsicht eines Bediensteten vorzunehmen, der die Befähigung zum Richteramt hat.

(2) Die Maßnahmen sind unverzüglich zu beenden, wenn sie nicht mehr erforderlich sind oder die Voraussetzungen der Anordnung nicht mehr vorliegen. Die Beendigung ist der Stelle, die die Anordnung getroffen hat, und dem nach § 2 Abs. 1 Satz 1 oder 3 Verpflichteten, dem die Anordnung mitgeteilt worden ist, anzuzeigen. Die Anzeige an den Verpflichteten entfällt, wenn die Anordnung ohne seine Mitwirkung ausgeführt wurde.

(3) Postsendungen, die zur Öffnung und Einsichtnahme ausgehändigt worden sind, sind dem Postverkehr unverzüglich wieder zuzuführen. Telegramme dürfen dem Postverkehr nicht entzogen werden. Der zur Einsichtnahme berechtigten Stelle ist eine Abschrift des Telegramms zu übergeben.

§ 12
Mitteilungen an Betroffene

(1) Beschränkungsmaßnahmen nach § 3 sind dem Betroffenen nach ihrer Einstellung mitzuteilen, wenn eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann. Lässt sich in diesem Zeitpunkt noch nicht beurteilen, ob diese Voraussetzung vorliegt, ist die Mitteilung vorzunehmen, sobald eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann. Einer Mitteilung bedarf es nicht, wenn die G 10-Kommission einstimmig festgestellt hat, dass

1. diese Voraussetzung auch nach fünf Jahren nach Beendigung der Maßnahme noch nicht eingetreten ist,

2. sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten wird und

1. die Voraussetzungen für eine Löschung sowohl bei der erhebenden Stelle als auch beim Empfänger vorliegen.

(2) Absatz 1 gilt entsprechend für Beschränkungsmaßnahmen nach den §§ 5 und 8, sofern die personenbezogenen Daten nicht unverzüglich gelöscht wurden. Die Frist von fünf Jahren beginnt mit der Erhebung der personenbezogenen Daten.

(3) Die Mitteilung obliegt der Behörde, auf deren Antrag die Anordnung ergangen ist. Wurden personenbezogene Daten übermittelt, erfolgt die Mitteilung im Benehmen mit dem Empfänger.

§ 13
Rechtsweg

Gegen die Anordnung von Beschränkungsmaßnahmen nach den §§ 3 und 5 Abs. 1 Satz 3 Nr. 1 und ihren Vollzug ist der Rechtsweg vor der Mitteilung an den Betroffenen nicht zulässig.

X

X

X

§ 17
Mitteilungsverbote

(1) Wird die Telekommunikation nach diesem Gesetz oder nach den §§ 100a, 100b der Strafprozessordnung überwacht, darf diese Tatsache von Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden.

(2) Wird die Aushändigung von Sendungen nach § 2 Abs. 1 Satz 1 oder 3 angeordnet, darf diese Tatsache von Personen, die zur Aushändigung verpflichtet oder mit der Sendungsübermittlung betraut sind oder hieran mitwirken, anderen nicht mitgeteilt werden.

(3) Erfolgt ein Auskunftsersuchen oder eine Auskunftserteilung nach § 2 Abs. 1, darf diese Tatsache oder der Inhalt des Ersuchens oder der erteilten Auskunft von Personen, die zur Beantwortung verpflichtet oder mit der Beantwortung betraut sind oder hieran mitwirken, anderen nicht mitgeteilt werden.

§ 18
Straftaten

Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 17 eine Mitteilung macht.

§ 19
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer

1. einer vollziehbaren Anordnung nach § 2 Abs. 1 Satz 1 oder 3 zuwiderhandelt,
2. entgegen § 2 Abs. 2 Satz 2 eine Person betraut oder
3. entgegen § 2 Abs. 2 Satz 3 nicht sicherstellt, dass eine Geheimschutzmaßnahme getroffen wird.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu dreißigtausend Deutsche Mark geahndet werden.

(3) Bußgeldbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die nach § 10 Abs. 1 zuständige Stelle.

X
X
X

§ 21
Einschränkung von Grundrechten

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird durch dieses Gesetz eingeschränkt.

IV.4 Auszug aus dem Außenwirtschaftsgesetz (AWG)

§ 39
Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses

(1) Zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz oder dem Kriegswaffenkontrollgesetz ist das Zollkriminalamt berechtigt, dem Brief-, Post- oder Fernmeldegeheimnis unterliegende Sendungen zu öffnen und einzusehen sowie die Telekommunikation einschließlich der dazu nach Wirksamwerden der Anordnung (§ 40) innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte zu überwachen und aufzuzeichnen. Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird insoweit eingeschränkt.

(2) Beschränkungen nach Absatz 1 dürfen nur angeordnet werden gegenüber

1. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung nach § 34 Abs. 1 bis 6, auch in Verbindung mit § 35, dieses Gesetzes oder § 19 Abs. 1 bis 3, § 20 Abs. 1 und 2, jeweils auch in Verbindung mit § 21, oder § 22a Abs. 1 Nr. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen planen,

2. einer natürlichen oder juristischen Person oder einer Personenvereinigung, wenn eine der in Nummer 1 bezeichneten Personen für sie tätig ist und eine Maßnahme nach Nummer 1 nicht ausreicht, oder

3. anderen Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für eine in Nummer 1 bezeichnete Person bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben oder dass eine solche Person ihren Anschluss benutzt.

Die Maßnahme nach Nummer 2 darf nur angeordnet werden, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person an dem Postverkehr der natürlichen oder juristischen Person oder Personenvereinigung teilnimmt oder deren Telekommunikationsanschluss benutzt.

(3) Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und die Maßnahme nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht. Die

Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(4) Vor dem Antrag auf Anordnung ist die Staatsanwaltschaft zu unterrichten. Ebenso ist die Staatsanwaltschaft von der richterlichen Entscheidung, von einer Entscheidung des Bundesministers der Finanzen bei Gefahr im Verzug und von dem Ergebnis der beantragten Maßnahme zu unterrichten.

(5) Artikel 1 § 1 Abs. 2 bis 4 des Gesetzes zu Artikel 10 Grundgesetz gilt entsprechend.

§ 40
Richterliche Anordnung

(1) Beschränkungen nach § 39 Abs. 1 sind vom Behördenleiter oder dessen Stellvertreter unter Angabe von Art, Umfang und Dauer der beantragten Maßnahme nach Zustimmung des Bundesministers der Finanzen schriftlich zu beantragen und zu begründen. In dem Antrag ist darzulegen, dass die in § 39 Abs. 3 Satz 1 bezeichneten Voraussetzungen vorliegen.

(2) Die Anordnung ergeht durch das Landgericht, bei Gefahr im Verzug durch den Bundesminister der Finanzen. Die Anordnung des Bundesministers der Finanzen tritt außer Kraft, wenn sie nicht binnen drei Tagen von dem Landgericht bestätigt wird.

(3) Zuständig ist das Landgericht, in dessen Bezirk das Zollkriminalamt seinen Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(4) Die Anordnung ergeht schriftlich. Sie muss Namen und Anschrift des Betroffenen enthalten, gegen den sie sich richtet. In ihr sind Art, Umfang und Dauer der Maßnahme zu bestimmen, bei einer Überwachung der Telekommunikation auch die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die in § 39 bezeichneten Voraussetzungen fortbestehen.

§ 41
Durchführungsvorschriften

(1) Die aus der Anordnung sich ergebenden Maßnahmen nach § 39 Abs. 1 sind unter Verantwortung des Zollkriminalamtes und unter Aufsicht eines Bediensteten vorzunehmen, der die Befähigung zum Richteramt hat. Artikel 1 § 7 Abs. 2 und § 8 des Gesetzes zu Artikel 10 Grundgesetz ist entsprechend anzuwenden.

(2) Die durch die Maßnahmen erlangten personenbezogenen Daten dürfen von öffentlichen Stellen nur zu Verhütung oder Aufklärung der in § 39 Abs. 1 dieses Gesetzes und Artikel 1 § 2 Abs. 1 und § 3 Abs. 3 des Gesetzes zu Artikel 10 Grundgesetz genannten Straftaten verarbeitet und genutzt werden, soweit sich bei Gelegenheit der Auswertung Tatsachen ergeben, die die Annahme rechtfertigen, dass eine solche Straftat begangen werden soll, begangen wird oder begangen worden ist.

(3) Sind die durch die Maßnahmen erlangten Unterlagen über einen am Postverkehr oder an der Telekommunikation Beteiligten zu den in Absatz 2 genannten Zwecken nicht mehr erforderlich, sind sie unter Aufsicht eines der in Absatz 1 genannten Bediensteten unverzüglich zu vernichten. Über die Vernichtung ist eine Niederschrift anzufertigen. Zur Sicherung der ordnungsgemäßen Vernichtung sind in regelmäßigen Abständen Prüfungen durchzuführen.

(4) Von den getroffenen Maßnahmen ist der Betroffene durch das Zollkriminalamt zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahme geschehen kann. Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden, entscheidet die Staatsanwaltschaft über den Zeitpunkt der Unterrichtung.

(5) Der Bundesminister der Finanzen unterrichtet in Abständen von höchstens sechs Monaten ein Gremium, das aus neun vom Bundestag bestimmten Abgeordneten besteht, über die Durchführung der §§ 39 bis 43 dieses Gesetzes.

§ 42
Verschiegenheitspflicht

(1) Werden Beschränkungen nach den §§ 39 bis 41 vorgenommen, so darf diese Tatsache von Personen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen Absatz 1 eine Mitteilung macht.

Anhang 2

Fangschaltungsbeschluss des Bundesverfassungsgerichts

Beschluss des Bundesverfassungsgerichts vom 25. März 1992 - 1 BvR 1430/88 - („Fangschaltungsbeschluss“)

Leitsätze:

1. Sämtliche der Post zur Beförderung oder Übermittlung anvertrauten Kommunikationsvorgänge und -inhalte genießen den Schutz des Art. 10 Abs. 1 GG.

2. Die Erfassung von Ferngesprächsdaten mittels Fangschaltungen und Zählervergleichseinrichtungen durch die Deutsche Bundespost greift in das Grundrecht aus Art. 10 Abs. 1 GG ein und bedarf einer gesetzlichen Grundlage.

3. § 30 Abs. 2 PostVerfassungsgesetz bildet keine ausreichende gesetzliche Ermächtigung zum Erlass von Regelungen über Fangschaltungen und Zählervergleichseinrichtungen.

(Beschlusstext siehe Sammlung der Entscheidungen des Bundesverfassungsgerichts Band 85 Seite 386)

Anhang 3

Guidelines zur Kundeninformation

1. Datenverarbeitungstatbestände

Dem Kunden sollte erläutert werden, dass bestimmte personenbezogene Daten (Bestandsdaten) für die Begründung und Änderung des Kundenverhältnisses erforderlich sind, wie z.B. Name, Anschrift, Geburtsdatum. Auch die Löschung dieser Daten mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres sollte erwähnt werden. Bereits auf dem Formular muss deutlich erkennbar sein, dass weitergehende Angaben (z.B. zum Beruf) auf freiwilliger Basis erfolgen.

In diesem Zusammenhang sollten die verschiedenen Datenarten (Bestands-, Verbindungsdaten), die für das Vertragsverhältnis entscheidend sind, benannt und erläutert werden.

Im Rahmen der Verbindungsdaten muss dem Kunden erläutert werden, dass die Rufnummern des anrufenden und des angerufenen Anschlusses, die in Anspruch genommene Dienstleistung sowie Beginn und Ende der Verbindung für die Rechnungserstellung gespeichert werden. Auf die Speicherfrist von höchstens sechs Monaten nach Versendung der Rechnung bei Kürzung der Zielrufnummer um die letzten drei Ziffern sollte hingewiesen werden. Auch die Möglichkeit, diese Daten auf Antrag sofort mit Rechnungsversand löschen zu lassen bzw. diese vollständig zu speichern müsste erwähnt werden. Diese Wahlmöglichkeiten müssen auch in das Formular aufgenommen werden.

Außerdem sollte der Kunde darüber informiert werden, dass in den Fällen einer sog. Flatrate oder wenn die Nutzung des Anschlusses zu bestimmten Zeiten umsonst ist, keine Verbindungsdaten gespeichert werden.

Eine Information über die Weitergabe der Verbindungsdaten für die Abrechnung mit anderen Diensteanbietern oder mit deren Kunden kann aufgenommen werden.

Es kann eine Information darüber erfolgen, dass die Verbindungsdaten sowohl zum Erkennen und zur Beseitigung von Störungen und Fehlern an Telekommunikationsanlagen als auch zur Erkennung und Unterbindung von Leistungserschleichungen genutzt werden dürfen.

2. Einwilligung (§ 89 Abs. 10 TKG, §§ 3, 4 TDSV)

In einigen Fällen ist die Einwilligung Voraussetzung für die Datenverarbeitung (z.B. EVN). Diese bedarf grundsätzlich der Schriftform, so dass alle Datenverarbeitungstatbestände, für die eine Einwilligung erforderlich ist, auf den Formularen aufgeführt werden müssen. Falls ein entsprechender Auftrag über ein Call-Center erteilt wird, muss der Kunde darüber informiert sein, dass dieser erst nach einem entsprechenden Bestätigungsschreiben ausgeführt werden kann.

Wichtig ist der Hinweis, dass ein Kunde auch eine erteilte Einwilligung jederzeit für die Zukunft wieder zurücknehmen kann.

Die Möglichkeit der elektronischen Einwilligung muss erläutert werden. Der Kunde sollte darüber informiert werden:

- wie die Einwilligung im Rahmen der Website des Unternehmens erteilt wird;

- dass die Einwilligung vom TK-Unternehmen protokolliert wird;

- wie der Inhalt der Einwilligung wieder abgerufen werden kann;

- dass eine Rücknahmemöglichkeit innerhalb einer Woche besteht und wie diese erfolgen kann.

3. Einzelverbindungsnachweis (§ 89 Abs. 2 Nr. 3 a TKG, § 8 TDSV i.V.m. § 7 Abs. 3,4 TDSV)

Dem Kunden sollte dargelegt werden, dass ein Einzelverbindungsnachweis nur auf schriftlichen Antrag hin für die Zukunft erstellt wird, aus diesem Grund muss dieser Bereich auch im Antragsformular aufgeführt werden. Auf die dafür notwendige Mitbenutzerklärung/Beteiligung der Personalvertretung (des Betriebsrates) - die bereits im Formular enthalten sein muss - sollte nochmals erläuternd eingegangen werden.

Es sollte ein Hinweis darauf erfolgen, dass Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen nicht im EVN erscheinen, die grundsätzlich anonym bleibenden Anrufern Beratung in seelischen und sozialen Notlagen anbieten.

4. Kundenverzeichnisse/Auskunft (§§ 13,14 TDSV)

Den Kunden muss klar dargelegt werden, dass sie bestimmen können, ob und mit welchen Angaben (z.B. Name, Anschrift, zusätzliche Angaben wie Beruf, Branche und Art des Anschlusses) sie in öffentliche Verzeichnisse eingetragen werden. Dass Mitbenutzer eingetragen werden können, wenn diese damit einverstanden sind, sollte erwähnt werden.

Außerdem ist es wichtig, die Wahlmöglichkeiten darzustellen, ob die gewählten Angaben nur in gedruckte (Telefonbücher etc.), nur in elektronische (z.B. CD-ROM´s) oder sowohl in gedruckte als auch elektronische Verzeichnisse eingetragen werden sollen.

Dem Kunden sollte erläutert werden, dass Diensteanbieter im Rahmen von Auskunftsdiensten im Einzelfall Auskunft über in den o.g. Verzeichnissen enthaltene Daten erteilen oder durch Dritte erteilen lassen dürfen, soweit der Beauskunftung nicht widersprochen wurde.

5. Werbung, Kundenberatung, Marktforschung (§ 5 Abs. 2 TDSV)

Die Tatsache, dass Bestandsdaten zur Werbung, Beratung und zur Marktforschung nur verarbeitet und genutzt werden dürfen, wenn der Kunde eine Einwilligung erteilt hat, muss erläutert werden. Diese Fragestellung muss bereits im Formular Aufnahme finden. Auf die Möglichkeit, die erteilte Einwilligung jederzeit für die Zukunft widerrufen zu können, sollte hingewiesen werden.

6. Bonitätsprüfung

Fast alle TK-Unternehmen führen Bonitätsprüfungen ihrer Kunden bei der SCHUFA oder anderen Wirtschaftsauskunfteien durch. Die Einwilligungserklärung dafür muss auf dem Formular enthalten sein. Nähere Erläuterungen müssen dem Kunden dann auf dem Informationsblatt oder einer gesonderten Anlage gegeben werden. Eine Erläuterung nur in den AGB genügt insoweit nicht. Diese Information muss die SCHUFA-Klausel in neuester Fassung und die Angabe der Anschrift der zuständigen SCHUFA enthalten. Auch die Wirtschaftsauskunfteien, bei denen die gleichen

Abfragen erfolgen und an die die gleichen Daten weitergegeben werden wie bei der SCHUFA, müssen namentlich genannt und die Anschrift muss mitgeteilt werden.

7. Rufnummernanzeige (§ 11 TDSV)

Wird für einen Anschluss die sog. Rufnummernanzeige (CLI) angeboten, so müssen die folgenden Möglichkeiten - soweit sie technisch möglich sind - erwähnt werden:

- für eingehende Anrufe kann die Anzeige der Nummer auf dem Display des Angerufenen dauernd oder im Einzelfall unterdrückt werden;

- bei abgehenden Anrufen kann die Anzeige der Rufnummer auf dem Display des Angerufenen dauernd oder im Einzelfall unterdrückt werden.

- Es besteht die Möglichkeit, eingehende Anrufe, bei denen die Rufnummernanzeige vom Anrufenden unterdrückt wurde, abzuweisen.

Es sollte darauf hingewiesen werden, dass bei abgehenden Anrufen die Anzeige der Nummer grundsätzlich unterbleibt, wenn keine Eintragung von Angaben in ein Kundenverzeichnis beantragt wurde. Es kann jedoch ausdrücklich bestimmt werden, dass auch ohne eine Eintragung in Verzeichnisse die Rufnummer beim Angerufenen angezeigt wird.

Es muss darauf hingewiesen werden, dass bei der Versendung von SMS die Rufnummer als Bestandteil der Absenderadresse immer mit übertragen wird.

8. Rechnungserstellung im Ausland (§ 3 Abs. 5 TDSV i.V.m. BDSG)

Wenn die Rechnung im Ausland erstellt wird, muss ein Hinweis aufgenommen werden, dass die Verbindungsdaten ins Ausland übermittelt werden und um welches Land es sich handelt. Es kann vermerkt werden, dass die Verantwortlichkeit für diese Datenverarbeitung im Ausland beim TK-Unternehmen verbleibt.

9. Anrufweiterschaltung (§ 12 TDSV)

Der Kunde soll darauf hingewiesen werden, dass die von einem Dritten veranlasste Weiterschaltung eines Anrufs auf das Endgerät von ihm abgestellt werden kann (soweit dies technisch möglich ist).

10. Auskunfts- und Berichtigungsrecht (§§ 34, 35 BDSG)

Der Kunde sollte darauf hingewiesen werden, dass er jederzeit kostenlos Auskunft über den Umfang und Zweck der über ihn gespeicherten Daten, die Weitergabe an Dritte und den Ursprung der Daten erhalten kann.

Es sollte deutlich gemacht werden, dass auf Grund eines Hinweises des Kunden unrichtige Daten umgehend berichtigt werden.

11. Weitergabe von Bestands- und Verbindungsdaten an Dritte

Der Kunde sollte darüber informiert werden, dass diese Daten an Dritte weitergegeben werden, falls zur Durchsetzung der Forderungen ein Dritter beauftragt wurde.

In den Fällen, in denen der Diensteanbieter Produkte und Dienstleistungen eines Dritten über die Telekommunikationsrechnung abrechnet, sollte ein Hinweis erfolgen, dass diesen Dritten Bestands- und Verbindungsdaten im Einzelfall übermittelt werden dürfen, soweit dies zur Durchsetzung ihrer Forderungen erforderlich ist.

12. Hinweis auf § 12 TKG

Die Verpflichtung, Kundendaten an Dritte weitergeben zu müssen, die Kundenverzeichnisse herausgeben oder einen Auskunftsdienst aufnehmen wollen, kann dargelegt werden. Dabei muss dann deutlich gemacht werden, dass die Wünsche des Kunden bezüglich des Eintrags in gedruckte oder elektronische Verzeichnisse bzw. zur Aufnahme in die Auskunft beachtet werden.

13. Mailbox (§ 16 TDSV)

Nachrichteninhalte dürfen grundsätzlich nicht gespeichert werden. Eine Ausnahme besteht nur in den Fällen, in denen gerade die Aufzeichnung Teil des angebotenen Dienstes ist. Dieser Hinweis kann in die Erläuterungen aufgenommen werden.

Anhang 4

SCHUFA-Klausel zu Telekommunikationsanträgen

Ich willige ein, dass die Firma[1] der SCHUFA Holding AG, Hagenauer Strasse 44, 54203 Wiesbaden, Daten über die Beantragung, Aufnahme und Beendigung dieses Telekommunikationsvertrages übermittelt und Auskünfte über mich von der SCHUFA erhält.

Unabhängig davon wird die Firma[1] der SCHUFA auch Daten aufgrund nichtvertragsgemäßen Verhaltens (z. B. Forderungsbetrag nach Kündigung, Kartenmissbrauch) übermitteln. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies nach Abwägung aller betroffenen Interessen zulässig ist.

Die SCHUFA speichert und übermittelt die Daten an ihre Vertragspartner im EU-Binnenmarkt, um diesen Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen Personen zu geben. Vertragspartner der SCHUFA sind vor allem Kreditinstitute, Kreditkarten- und Leasinggesellschaften. Daneben erteilt die SCHUFA Auskünfte an Handels-, Telekommunikations- und sonstige Unternehmen, die Leistungen und Lieferungen gegen Kredit gewähren. Die SCHUFA stellt personenbezogene Daten nur zur Verfügung, wenn ein berechtigtes Interesse hieran im Einzelfall glaubhaft dargelegt wurde. Zur Schuldnerermittlung gibt die SCHUFA Adressdaten bekannt. Bei der Erteilung von Auskünften kann die SCHUFA ihren Vertragspartnern ergänzend einen aus ihrem Datenbestand errechneten Wahrscheinlichkeitswert zur Beurteilung des Kreditrisikos mitteilen (Score-Verfahren).

Ich kann Auskunft bei der SCHUFA über die mich betreffenden gespeicherten Daten erhalten. Weitere Informationen über das SCHUFA-Auskunfts- und Score-Verfahren enthält ein Merkblatt, das auf Wunsch zur Verfügung gestellt wird. Die Adresse der SCHUFA lautet:

SCHUFA Holding AG, Verbraucherservice, Postfach 600509, 44845 Bochum
SCHUFA Holding AG, Verbraucherservice, Postfach 5640, 30056 Hannover

---
Unterschrift

_____

[1] zu personalisieren

Anhang 5

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (luK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z.B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der luK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie lässt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von luK-Systemen ebenso stark beeinflusst wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne dass die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem

Begriff "Privacy enhancing technology (PET)" eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfasst, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, dass er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, dass sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit lässt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Be-reitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, dass die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm "Forschung und Entwicklung" aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Anhang 6

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- **Erhebliche Zunahme der Telekommunikationsvorgänge**
  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mailboxen sowie das Internet genutzt.

- **Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten**

  - Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.
  - Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.
  - Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.
  - Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.
  - Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres

Standorts.

- **Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten**
  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

- **Entwicklung des Internets zum Massenkommunikationsmittel**
  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

- **Schwer durchschaubare Rechtslage**
  Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802

- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.

- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe,

Behörden oder möglicherweise sogar Krankenhäuser betreffen.

- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen “ENFOPOL”, befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.

- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.

- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.

- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.

- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.

- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselungvon elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine

Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.

- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.

Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

Anhang 7

Entschließung
zwischen der 61. und 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vom 10.Mai 2001)

Zum Entwurf der Telekommunikations-Überwachungsverordnung

Das Bundesministerium für Wirtschaft hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung (TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Begriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße "Surfen" zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht,

G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.

Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

Anhang 8

Weitere Informationsschriften des BfD zum Datenschutz

Beim Bundesbeauftragten für den Datenschutz können folgende Schriften kostenlos angefordert werden:

- **BfD-Info 1 - Bundesdatenschutzgesetz - Text und Erläuterung -**
  Die Broschüre enthält den Gesetzestext und erläutert die Gesetzesvorschriften

- **BfD-Info 2 - Der Bürger und seine Daten -**
  Die Broschüre gibt einen Überblick über die Stellen, die möglicherweise personenbezogene Daten über Sie erheben, verarbeiten und nutzen und bei denen Sie Ihre Datenschutzrechte geltend machen können.

- **BfD-Info 3 - Schutz der Sozialdaten -**
  Die Broschüre stellt den besonderen Datenschutz im Bereich der Sozialversicherung - also der Kranken-, Unfall- und Rentenversicherung sowie der Arbeitslosen- und der Pflegeversicherung - und auch anderer Sozialleistungen, wie z.B. Sozialhilfe, nach dem Sozialgesetzbuch dar.

- **BfD-Info 4 - Der behördliche Datenschutzbeauftragte -**
  Die Broschüre informiert über Bestellung, Befugnisse und Aufgaben des behördlichen Datenschutzbeauftragten

- **Tätigkeitsberichte soweit vorhanden**
  Ab dem 16. Tätigkeitsbericht (für die Jahre 1995 und 1996) sind diese auch auf CD-ROM erhältlich.
  Neben dem aktuellen Tätigkeitsbericht, der auf der CD-ROM in verschiedenen Formaten - HTML, WINWORD 2.0 und 6.0, RTF sowie im ASCII-Code - angeboten wird, befinden sich darauf auch die Informationsbroschüren BfD-INFO 1 bis BfD-INFO 5 im WINWORD-Format sowie ein Browser.

- **Bundesdatenschutzgesetz** in **englischer** Sprache

- **Bundesdatenschutzgesetz** in **französischer** Sprache

Die vorgenannten Broschüren und Texte sind auch im Internetangebot des Bundesbeauftragten für den Datenschutz unter der Adresse http://www.datenschutz.bund.de enthalten (vgl. Anhang 9).

Anhang 9

Elektronische Informationen zum Datenschutz

Vor dem Hintergrund der steigenden Bedeutung des Internets als Kommunikationsmedium ist der Bundesbeauftragte für den Datenschutz auch dort mit einem Angebot vertreten. Die Homepage ist unter der Adresse http://www.datenschutz.bund.de erreichbar. Das Angebot umfasst neben den Rubriken „Bürger fragen“ und „Datenschutz von A-Z“ u.a.

- aktuelle Hinweise und Pressemitteilungen zum Datenschutz,
- umfangreiche Materialien wie Tätigkeitsberichte, alle BfD-Informationsbroschüren, Gesetzes- und Verordnungstexte (z.T. auch in englischer Sprache), Entschließungen der Datenschutzkonferenzen,
- Informationen zum europäischen Datenschutz und die internationale Zusammenarbeit der Datenschutzbeauftragten,
- Informationen zum Thema „Datenschutz und Technik“, darunter ein Beitrag „Datenschutzfreundliche Technologien in der Telekommunikation“
- Anschriften und weitere interessante Links.

Daneben können Informationen zum Datenschutz auch beim **Virtuellen Datenschutzbüro** unter der Adresse http://www.datenschutz.de abgerufen werden. Das Projekt „Virtuelles Datenschutzbüro“ wurde vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein initiiert und aufgebaut. Es ist Portal und Ansprechstelle im Internet für alle Bürgerinnen und Bürger, Experten und Datenschutzinstitutionen. Projektpartner sind neben dem Bundesbeauftragten für den Datenschutz auch die Datenschutzbeauftragten der meisten Bundesländer, die Norddeutschen Bistümer der Katholischen Kirche und Datenschutzbeauftragte aus der Schweiz, den Niederlanden und Kanada.
Die seit Ende 2000 bestehende neue Einrichtung bietet u.a.:

- Informationen zu allen Fragen rund um den Datenschutz,
- Diskussionsforen zu aktuellen Datenschutzthemen,
- Antworten zu den häufigsten Fragen von Anwendern,
- Eine Plattform für die Zusammenarbeit der Datenschützer weltweit.

Anhang 10

Anschriften der Datenschutzbeauftragten des Bundes und der Länder

Bund	Der Bundesbeauftragte für den Datenschutz	Peter Schaar Postfach 200112 53131 Bonn Husarenstraße 30 53117 Bonn	Tel.: 0228/81995-0 Fax: 0228/81995-550 e-mail: poststelle@bfd.bund.de Internet: http://www.bfd.bund.de
Baden-Württemberg	Der Landesbeauftragte für den Datenschutz Baden-Württemberg	Peter Zimmermann Postfach 102932 70025 Stuttgart Urbanstr. 32 70182 Stuttgart	Tel.: 0711/615541-0 Fax: 0711/615541-15 e-mail: poststelle@lfd.bwl.de Internet: http://www.baden-wuerttemberg.datenschutz.de
Bayern	Der Bayerische Landesbeauftragte für den Datenschutz	Reinhard Vetter Postfach 221219 80502 München Wagmüllerstr. 18 80538 München	Tel.: 089/212672-0 Fax: 089/212672-50 e-mail: poststelle@datenschutz-bayern.de Internet: http://www.datenschutz-bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit	Prof. Dr. Hansjürgen Garstka An der Urania 4-10 10787 Berlin	Tel.: 030/13889-0 Fax: 030/2155050 e-mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de
Brandenburg	Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht	Dr. Alexander Dix Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 033203/356-0 Fax: 033203/356-49 e-mail: poststelle@lda.brandenburg.de Internet: http://www.lda.brandenburg.de
Bremen	Landesbeauftragter für den Datenschutz	Sven Holst Postfach 100380 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven	Tel.: 0471/924610 Fax: 0471/9246131 e-mail: office@datenschutz.bremen.de Internet: http://datenschutz.-bremen.de
Hamburg	Der Hamburgische Datenschutzbeauftragte	Dr. Hans-Hermann Schrader Baumwall 7 20459 Hamburg	Tel.: 040/42841-2044 Fax: 040/42841-2372 e-mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg.datenschutz.de
Hessen	Der Hessische Datenschutzbeauftragte	Prof. Dr. Michael Ronellenfitsch Postfach 3163 65021 Wiesbaden Uhlandstr. 4 65189 Wiesbaden	Tel.: 0611/1408-0 Fax: 0611/1408-900 e-mail: poststelle@datenschutz.hessen.de Internet: http://www.datenschutz.hessen.de
Mecklenburg-Vorpommern	Landesbeauftragter für den Datenschutz	Dr. Werner Kessel Schloss Schwerin 19053 Schwerin	Tel.: 0385/59494-0 Fax: 0385/59494-58 e-mail: datenschutz@mvnet.de Internet: http://www.lfd.m-v.de
Niedersachsen	Der Landesbeauftragte für den Datenschutz Niedersachsen	Burckhard Nedden Postfach 221 30002 Hannover Brühlstr. 9 30169 Hannover	Tel.: 0511/120-4500 Fax: 0511/120-4599 e-mail: mail@lfd.niedersachsen.de Internet: http://www.lfd.niedersachsen.de

Nordrhein-Westfalen	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen	Bettina Sokol Postfach 200444 40102 Düsseldorf Reichsstr. 43 40217 Düsseldorf	Tel.: 0211/384240 Fax: 0211/3842410 e-mail: poststelle@ldi.nrw.de Internet: http://www.ldi.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz	Prof. Dr. Walter Rudolf Postfach 3040 55020 Mainz Deutschhausplatz12 55116 Mainz	Tel.: 06131/2082449 Fax: 06131/2082497 e-mail: poststelle@datenschutz.rlp.de Internet: http://www.datenschutz.rlp.de
Saarland	Der Landesbeauftragte für Datenschutz	Karl Albert Postfach 102631 66026 Saarbrücken Fritz-Dobisch-Str. 12 66111 Saarbrücken	Tel.: 0681/94781-0 Fax: 0681/9478129 e-mail: lfd-saar@t-online.de Internet:: http://www.lfd.saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte	Andreas Schurig Postfach 120905 01008 Dresden Bernhard-von-Lindenau-Platz 1 01067 Dresden	Tel.: 0351/4935-401 Fax: 0351/4935-490 e-mail: saechsdsb@slt.sachsen.de Internet: http://www.datenschutz.sachsen.de
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt	Klaus-Rainer Kalk Postfach 1947 39009 Magdeburg Berliner Chaussee 9 39114 Magdeburg	Tel.: 0391/81803-0 Fax: 0391/81803-33 e-mail: poststelle@lfd.lsa-net.de Internet: http://www.datenschutz.sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Dr. Helmut Bäumler Postfach 7116 24171 Kiel Holstenstraße 98 24103 Kiel	Tel.: 0431/9881200 Fax: 0431/9881223 e-mail: mail@datenschutzzentrum.de Internet: http://www.datenschutzzentrum.de
Thüringen	Die Thüringer Landesbeauftragte für den Datenschutz	Silvia Liebaug Postfach 101951 99019 Erfurt Johann-Sebastian-Bach-Straße 1 99096 Erfurt	Tel.: 0361/3771900 Fax: 0361/3771904 e-mail: poststelle@datenschutz.thueringen.de Internet: http://www.datenschutz.thueringen.de

Anhang 11

Anschriften der Aufsichtsbehörden für den nicht öffentlichen Bereich

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Baden-Württemberg	Innenministerium Baden-Württemberg Postfach 10 24 43 70020 Stuttgart Dorotheenstr. 6 70173 Stuttgart Tel.: 0711/231-4 Fax: 0711/231-3299 E-Mail: poststelle@im.bwl.de Internet: www.im.baden-wuerttemberg.de	Innenministerium Baden-Württemberg Postfach 10 24 43 70020 Stuttgart Dorotheenstr. 6 70173 Stuttgart Tel.: 0711/231-4 Fax: 0711/231-3299 E-Mail: poststelle@im.bwl.de Internet: www.im.baden-wuerttemberg.de
Bayern	Bayerisches Staatsministerium des Innern Odeonsplatz 3 80539 München Tel.: 089/2192-01 Fax: 089/2192-12266	Regierung von Mittelfranken Aufsichtsbehörde für den Datenschutz Promenade 27 91522 Ansbach Tel.: 0981/53-0 Fax: 0981/53-1206 E-Mail: datenschutz@reg-mfr.bayern.de Internet: www.regierung.mittelfranken.bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4-10 10787 Berlin Tel.: 030/13889-0 Fax: 030/2155050 E-Mail:mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de	Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4-10 10787 Berlin Tel.: 030/13889-0 Fax: 030/2155050 E-Mail:mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de
Brandenburg	Ministerium des Innern Henning-von-Tresckow-Str. 9 - 13 14467 Potsdam Tel.: 0331/8662360 Fax: 0331/8662302 E-Mail: Datenschutz-Aufsicht-Bbg@t-online. de Internet:http://www.mi.brandenburg.de	Ministerium des Innern Henning-von-Tresckow-Str. 9 - 13 14467 Potsdam Tel.: 0331/8662360 Fax: 0331/8662302 E-Mail: Datenschutz-Aufsicht-Bbg@t-online. de Internet: http://www.mi.brandenburg.de
Bremen	Der Landesbeauftragte für den Datenschutz Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven Tel.: 0471/924610 Fax: 0471/9246131 E-Mail:office@datenschutz.bremen.de Internet: http://www.datenschutz.bremen.de	Der Landesbeauftragte für den Datenschutz Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven Tel.: 0471/924610 Fax: 0471/9246131 E-Mail: office@datenschutz.bremen.de Internet: http://www.datenschutz.bremen.de

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Hamburg	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg Tel.: 040/42841-2045 Fax: 040/42841-2372 E-Mail: mailbox@datenschutz.hamburg.de Internet: http://www.hamburg.datenschutz.de	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg Tel.: 040/42841-2045 Fax: 040/42841-2372 E-Mail: mailbox@datenschutz.hamburg.de Internet: http://www.hamburg.datenschutz.de
Hessen	Hessisches Ministerium des Innern und für Sport Friedrich-Ebert-Allee 12 65185 Wiesbaden Tel.: 0611/353-0 Fax: 0611/353-1343 Internet: http://www.hmdi.hessen.de	Regierungspräsidium Gießen Landgraf-Philipp-Platz 3-7 35390 Gießen Tel.: 0641/303-1 Fax: 0641/303-2509 Internet: http://www.rp-giessen.de Regierungspräsidium Darmstadt Wilhelminenstraße 1-3 64283 Darmstadt Tel.: 06151/12-0 Fax: 06151/12-6834 E-Mail: datenschutz@rpda.hessen.de Internet: http://www.rpda.de Regierungspräsidium Kassel Steinweg 6 34117 Kassel Tel.: 0561/106-0 Fax: 0561/106-1012 Internet: http://www.rp-kassel.de
Mecklenburg-Vorpommern	Innenministerium des Landes Mecklenburg-Vorpommern Arsenal am Pfaffenteich 19048 Schwerin Tel.: 0385/588-2250 Fax: 0385/588-2978	Innenministerium des Landes Mecklenburg-Vorpommern Arsenal am Pfaffenteich 19048 Schwerin Tel.: 0385/588-2250 Fax: 0385/588-2978
Niedersachsen	Niedersächsisches Ministerium für Inneres und Sport Lavesallee 6 30169 Hannover Tel.: 0511/120-0 Fax: 0511/120-6550	Der Landesbeauftragte für den Datenschutz Niedersachsen Postfach 2 21 30002 Hannover Brühlstraße 9 30169 Hannover Tel.: 0511/1204500 Fax: 0511/1204599 E-Mail: poststelle@lfd.niedersachsen.de Internet: http://www.lfd.niedersachsen.de
Nordrhein-Westfalen	Innenministerium des Landes Nordrhein-Westfalen	Landesbeauftragte für den Datenschutz und Informationsfreiheit

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
	Haroldstr. 5 40213 Düsseldorf Tel.: 0211/87101 Fax: 0211/8713355	Nordrhein-Westfalen Postfach 20 04 44 40102 Düsseldorf Reichsstraße 43 40217 Düsseldorf Tel.: 0211/384240 Fax: 0211/3842410 E-Mail: poststelle@ldi.nrw.de Internet: http://www.ldi.nrw.de
Rheinland-Pfalz	Ministerium des Innern und für Sport Schillerplatz 3 - 5 55116 Mainz Tel.: 06131/163259 Fax: 06131/163369	Aufsichts- und Dienstleistungsdirektion (ADD) Trier Willy-Brandt-Platz 3 54290 Trier Tel.: 0651/9494-0 Fax: 0651/9494-170 E-Mail: poststelle@add.rlp.de Internet: http://www.add.rlp.de
Saarland	Ministerium des Innern und für Sport Abt. B Mainzer Str. 136 66121 Saarbrücken Tel.: 0681/962-0 Fax: 0681/962-1605	Ministerium des Innern und für Sport Abt. B Mainzer Str. 136 66121 Saarbrücken Tel.: 0681/962-0 Fax: 0681/962-1605
Sachsen	Sächsisches Staatsministerium des Innern Referat 26 - Datenschutz Wilhelm-Buck-Straße 2 01097 Dresden Tel.: 0351/564-3260 Fax: 0351/564-3199 E-Mail: datenschutz@smi.sachsen.de	Regierungspräsidium Chemnitz Altchemnitzer Str. 41 09120 Chemnitz Tel.: 0371/532-1149 Fax: 0371/532-1159 E-Mail: post@rpc.sachsen.de Regierungspräsidium Dresden Stauffenbergallee 2 01099 Dresden Tel.: 0351/825-1420 Fax: 0351/825-9999 Regierungspräsidium Leipzig Braustr. 2 04107 Leipzig Tel.: 0341/977-1470 Fax: 0341/977-1199
Sachsen-Anhalt	Ministerium des Innern des Landes Sachsen-Anhalt Halberstädter Str. 2 39112 Magdeburg Tel.: 0391/5675404 Fax: 0391/5675290	Regierungspräsidium Halle Postfach 20 02 56 06003 Halle Willy-Lohmann-Str. 7 06114 Halle Tel.: 0345/5140 Fax: 0345/5141444 E-Mail: poststelle@rph.mi.lsa-net.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
	Holstenstraße 98 24103 Kiel Tel.: 0431/9881200 Fax: 0431/9881223 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de	Holstenstraße 98 24103 Kiel Tel.: 0431/9881200 Fax: 0431/9881223 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Thüringer Innenministerium Steigerstr. 24 99096 Erfurt Tel.: 0361/37-900 Fax: 0361/37-93449 E-Mail: poststelle@tim.thueringen.de	Thüringer Landesverwaltungsamt Weimarplatz 4 99423 Weimar Tel.: 0361/37-737258 Fax: 0361/37-737346 E-Mail: poststelle@tlva.thueringen.de

Stichwortverzeichnis

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)

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 sicherstellen, um in der Gemeinschaft den freien Verkehr personenbezogener Daten zu gewährleisten.

(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die Charta der Grundrechte der Europäischen Union anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 jener Charta niedergelegten Rechte uneingeschränkt geachtet werden.

(3) Die Vertraulichkeit der Kommunikation wird nach den internationalen Menschenrechtsübereinkünften, insbesondere der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, und den Verfassungen der Mitgliedstaaten garantiert.

(4) Mit der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation [5] wurden die Grundsätze der Richtlinie 95/46/EG in spezielle Vorschriften für den Telekommunikationssektor umgesetzt. Die 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 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.

---

[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 vom 14.5.2002, 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.
[5] ABl. L 24 vom 30.1.1998, S. 1.

(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 können auch das Format betreffen, in dem die Nachricht über das Netz weitergeleitet wird.

(16) Eine Information, die als Teil eines Rundfunkdienstes über ein öffentliches Kommunikationsnetz weitergeleitet wird, ist für einen potenziell unbegrenzten Personenkreis bestimmt und stellt keine Nachricht im Sinne dieser Richtlinie dar. Kann jedoch ein einzelner Teilnehmer oder Nutzer, der eine derartige Information erhält, beispielsweise durch einen Videoabruf-Dienst identifiziert werden, so ist die weitergeleitete Information als Nachricht im Sinne dieser Richtlinie zu verstehen.

(17) Für die Zwecke dieser Richtlinie sollte die Einwilligung des Nutzers oder Teilnehmers unabhängig davon, ob es sich um eine natürliche oder eine juristische Person handelt, dieselbe Bedeutung haben wie der in der Richtlinie 95/46/EG definierte und dort weiter präzisierte Begriff „Einwilligung der betroffenen Person“. Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website.

(18) Dienste mit Zusatznutzen können beispielsweise die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen umfassen.

(19) Die Anwendung bestimmter Anforderungen für die Anzeige des rufenden und angerufenen Anschlusses sowie für die Einschränkung dieser Anzeige und für die automatische Weiterschaltung zu Teilnehmeranschlüssen, die an analoge Vermittlungen angeschlossen sind, sollte in besonderen Fällen nicht zwingend vorgeschrieben werden, wenn sich die Anwendung als technisch nicht machbar erweist oder einen unangemessen hohen wirtschaftlichen Aufwand erfordert. Für die Beteiligten ist es wichtig, in solchen Fällen in Kenntnis gesetzt zu werden, und die Mitgliedstaaten müssen sie deshalb der Kommission anzeigen.

(20) Diensteanbieter sollen geeignete Maßnahmen ergreifen, um die Sicherheit ihrer Dienste, erforderlichenfalls zusammen mit dem Netzbetreiber, zu gewährleisten, und die 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 Einsatz spezieller Software oder von Verschlüsselungstechniken. Die Anforderung, die Teilnehmer über besondere Sicherheitsrisiken aufzuklären, entbindet einen Diensteanbieter nicht von der Verpflichtung, auf eigene Kosten unverzüglich geeignete Maßnahmen zu treffen, um einem neuen, unvorhergesehenen Sicherheitsrisiko vorzubeugen und den normalen Sicherheitsstandard des Dienstes wiederherzustellen. Abgesehen von den nominellen Kosten, die dem Teilnehmer bei Erhalt oder Abruf der Information entstehen, beispielsweise durch das Laden einer elektronischen Post, sollte die Bereitstellung der Informationen über Sicherheitsrisiken für die Teilnehmer kostenfrei sein. Die Bewertung der Sicherheit erfolgt unter Berücksichtigung des Artikels 17 der Richtlinie 95/46/EG.

(21) Es sollten Maßnahmen getroffen werden, um den unerlaubten Zugang zu Nachrichten — und zwar sowohl zu ihrem Inhalt als auch zu mit ihnen verbundenen Daten — zu verhindern und so die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen elektronischen Kommunikationsdiensten erfolgenden Nachrichtenübertragung zu schützen. Nach dem Recht einiger Mitgliedstaaten ist nur der absichtliche unberechtigte Zugriff auf die Kommunikation untersagt.

(22) Mit dem Verbot der Speicherung von Nachrichten und zugehörigen Verkehrsdaten durch andere Personen als die Nutzer oder ohne deren Einwilligung soll die automatische, einstweilige und vorübergehende Speicherung dieser Informationen insoweit nicht untersagt werden, als diese Speicherung einzig und allein zum Zwecke der Durchführung der Übertragung in dem elektronischen Kommunikationsnetz erfolgt und als die Information nicht länger gespeichert wird, als dies für die Übertragung und zum Zwecke der Verkehrsabwicklung erforderlich ist, und die Vertraulichkeit der Nachrichten gewahrt bleibt. Wenn dies für eine effizientere Weiterleitung einer öffentlich zugänglichen Information an andere Empfänger des Dienstes auf ihr Ersuchen hin erforderlich ist, sollte diese Richtlinie dem nicht entgegenstehen, dass die Information länger gespeichert wird, sofern diese Information der Öffentlichkeit auf jeden Fall uneingeschränkt zugänglich wäre und Daten, die einzelne, die Information anfordernde Teilnehmer oder Nutzer betreffen, gelöscht würden.

(23) Die Vertraulichkeit von Nachrichten sollte auch im Rahmen einer rechtmäßigen Geschäftspraxis sichergestellt sein. Falls erforderlich und rechtlich zulässig, können Nachrichten zum Nachweis einer kommerziellen Transaktion aufgezeichnet werden. Diese Art der 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 erfüllen. 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") [1] 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 [2] gewährleistet, dass die aus Gründen des Datenschutzes erforderliche Einführung von technischen Merkmalen elektronischer Kommunikationsgeräte einschließlich der Software harmonisiert wird, damit sie der Verwirklichung des Binnenmarktes nicht entgegensteht.

(47) Das innerstaatliche Recht sollte Rechtsbehelfe für den Fall vorsehen, dass die Rechte der Benutzer und Teilnehmer nicht respektiert werden. Gegen jede — privatem oder öffentlichem Recht unterliegende — Person, die den nach dieser Richtlinie getroffenen einzelstaatlichen Maßnahmen zuwiderhandelt, sollten Sanktionen verhängt werden.

(48) Bei der Anwendung dieser Richtlinie ist es sinnvoll, auf die Erfahrung der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Datenschutzgruppe aus Vertretern der für den Schutz personenbezogener Daten zuständigen Kontrollstellen der Mitgliedstaaten zurückzugreifen.

(49) Zur leichteren Einhaltung der Vorschriften dieser Richtlinie bedarf es einer Sonderregelung für die Datenverarbeitungen, die zum Zeitpunkt des Inkrafttretens der nach dieser Richtlinie erlassenen innerstaatlichen Vorschriften bereits durchgeführt werden —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Geltungsbereich und Zielsetzung

(1) Diese Richtlinie dient der Harmonisierung der Vorschriften der Mitgliedstaaten, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

[1] ABl. L 178 vom 17.7.2000, S. 1.

[2] ABl. L 91 vom 7.4.1999, S. 10.

(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") [1] auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

a) „Nutzer" eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

b) „Verkehrsdaten" Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

c) „Standortdaten" Daten, die in einem elektronischen Kommunikationsnetz verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

d) „Nachricht" jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein elektronisches Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

e) „Anruf" eine über einen öffentlich zugänglichen Telefondienst aufgebaute Verbindung, die eine zweiseitige Echtzeit-Kommunikation ermöglicht;

f) „Einwilligung" eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG;

g) „Dienst mit Zusatznutzen" jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

h) „elektronische Post" jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.

Artikel 3

Betroffene Dienste

(1) Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft.

(2) Die Artikel 8, 10 und 11 gelten für Teilnehmeranschlüsse, die an digitale Vermittlungsstellen angeschlossen sind, und — soweit dies technisch machbar ist und keinen unverhältnismäßigen wirtschaftlichen Aufwand erfordert — für Teilnehmeranschlüsse, die an analoge Vermittlungsstellen angeschlossen sind.

(3) Die Mitgliedstaaten teilen der Kommission die Fälle mit, in denen eine Einhaltung der Anforderungen der Artikel 8, 10 und 11 technisch nicht machbar wäre oder einen unverhältnismäßigen wirtschaftlichen Aufwand erfordern würde.

Artikel 4

Betriebssicherheit

(1) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

(2) Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes die Teilnehmer über dieses Risiko und — wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt — über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten.

Artikel 5

Vertraulichkeit der Kommunikation

(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht — unbeschadet des Grundsatzes der Vertraulichkeit — der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.

[1] ABl. L 108 vom 24.4.2002, S. 33.

(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 Dienstanbieter 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 ([1]).

(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 ([2]) Maßnahmen getroffen werden, um sicherzustellen, dass Endgeräte in einer Weise gebaut sind, die mit dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist.

Artikel 15

Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

(2) Die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

(3) Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr.

Artikel 16

Übergangsbestimmungen

(1) Artikel 12 gilt nicht für Ausgaben von Teilnehmerverzeichnissen, die vor dem Inkrafttreten der nach dieser Richtlinie erlassenen innerstaatlichen Vorschriften bereits in gedruckter oder in netzunabhängiger elektronischer Form produziert oder in Verkehr gebracht wurden.

(2) Sind die personenbezogenen Daten von Teilnehmern von Festnetz- oder Mobil-Sprachtelefondiensten in ein öffentliches Teilnehmerverzeichnis gemäß der Richtlinie 95/46/EG und gemäß Artikel 11 der Richtlinie 97/66/EG aufgenommen worden, bevor die nach der vorliegenden Richtlinie erlassenen innerstaatlichen Rechtsvorschriften in Kraft treten, so können die personenbezogenen Daten dieser Teilnehmer in der gedruckten oder elektronischen Fassung, einschließlich Fassungen mit Umkehrsuchfunktionen, in diesem öffentlichen Verzeichnis verbleiben, sofern die Teilnehmer nach Erhalt vollständiger Informationen über die Zwecke und Möglichkeiten gemäß Artikel 12 nicht etwas anderes wünschen.

Artikel 17

Umsetzung

(1) Die Mitgliedstaaten setzen vor dem 31. Oktober 2003 die Rechtsvorschriften in Kraft, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

([1]) 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).
([2]) ABl. L 36 vom 7.2.1987. Beschluss zuletzt geändert durch die Beitrittsakte von 1994.

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.

Geschehen zu Brüssel am 12. Juli 2002.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
P. COX	T. PEDERSEN