Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten* (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz - TDDDG)

TDDDG

Ausfertigungsdatum: 23.06.2021

Vollzitat:

"Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 8 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist"

Stand: Zuletzt geändert durch Art. 8 G v. 6.5.2024 I Nr. 149

* Dieses Gesetz dient der Umsetzung der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37), die durch Artikel 2 der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. L 337 vom 18.12.2009, S. 11) geändert worden ist.

Fußnote

```
(+++ Textnachweis ab: 1.12.2021 +++)
(+++ Amtlicher Hinweis des Normgebers auf EG-Recht:
     Umsetzung der
       EGRL 58/2002            (CELEX Nr: 32002L0058) +++)
```

Das G wurde als Artikel 1 des G v. 23.6.2021 I 1982 vom Bundestag mit Zustimmung des Bundesrates beschlossen. Es ist gem. Art. 14 Abs. 1 dieses G am 1.12.2021 in Kraft getreten.

Überschrift, Kurzbezeichnung u. Buchstabenabkürzung: IdF d. Art. 8 Nr. 1 Buchst. a bis c G v. 6.5.2024 I Nr. 149 mWv 14.5.2024

Inhaltsübersicht

Teil 1

Allgemeine Vorschriften

§ 1 Anwendungsbereich des Gesetzes

§ 2 Begriffsbestimmungen

Teil 2

Datenschutz und Schutz der Privatsphäre in der Telekommunikation

Kapitel 1

Vertraulichkeit der Kommunikation

§ 3 Vertraulichkeit der Kommunikation – Fernmeldegeheimnis
§ 4 Rechte des Erben des Endnutzers und anderer berechtigter Personen
§ 5 Abhörverbot, Geheimhaltungspflicht der Betreiber von Funkanlagen
§ 6 Nachrichtenübermittlung mit Zwischenspeicherung
§ 7 Verlangen eines amtlichen Ausweises
§ 8 Missbrauch von Telekommunikationsanlagen

Kapitel 2

Verkehrsdaten, Standortdaten

§ 9 Verarbeitung von Verkehrsdaten
§ 10 Entgeltermittlung und Entgeltabrechnung
§ 11 Einzelverbindungsnachweis
§ 12 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten
§ 13 Standortdaten

Kapitel 3

Mitteilen ankommender
Verbindungen, Rufnummernanzeige und
-unterdrückung, automatische Anrufweiterschaltung

§ 14 Mitteilen ankommender Verbindungen
§ 15 Rufnummernanzeige und -unterdrückung
§ 16 Automatische Anrufweiterschaltung

Kapitel 4

Endnutzerverzeichnisse,
Bereitstellen von Endnutzerdaten

§ 17 Endnutzerverzeichnisse
§ 18 Bereitstellen von Endnutzerdaten

Teil 3

Datenschutz bei digitalen Diensten, Endeinrichtungen

Kapitel 1

Technische und
organisatorische Vorkehrungen,
Verarbeitung von Daten zum Zweck
des Jugendschutzes und zur Auskunftserteilung

§ 19 Technische und organisatorische Vorkehrungen
§ 20 Verarbeitung personenbezogener Daten Minderjähriger
§ 21 Bestandsdaten
§ 22 Auskunftsverfahren bei Bestandsdaten
§ 23 Auskunftsverfahren bei Passwörtern und anderen Zugangsdaten
§ 24 Auskunftsverfahren bei Nutzungsdaten

Kapitel 2

Endeinrichtungen

§ 25 Schutz der Privatsphäre bei Endeinrichtungen
§ 26 Anerkannte Dienste zur Einwilligungsverwaltung, Endnutzereinstellungen

Teil 4

Straf- und Bußgeldvorschriften und Aufsicht

§ 27 Strafvorschriften
§ 28 Bußgeldvorschriften
§ 29 Zuständigkeit, Aufgaben und Befugnisse der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
§ 30 Zuständigkeit, Aufgaben und Befugnisse der Bundesnetzagentur

Teil 1
Allgemeine Vorschriften

§ 1 Anwendungsbereich des Gesetzes

(1) Dieses Gesetz regelt

1. das Fernmeldegeheimnis, einschließlich des Abhörverbotes und der Geheimhaltungspflicht der Betreiber von Funkanlagen,
2. besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und digitalen Diensten,
3. die Anforderungen an den Schutz der Privatsphäre im Hinblick auf die Mitteilung ankommender Verbindungen, die Rufnummernunterdrückung und -anzeige und die automatische Anrufweiterschaltung,
4. die Anforderungen an die Aufnahme in Endnutzerverzeichnisse und die Bereitstellung von Endnutzerdaten an Auskunftsdienste, Dienste zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers und Anbieter von Endnutzerverzeichnissen,

5. die von Anbietern von digitalen Diensten zu beachtenden technischen und organisatorischen Vorkehrungen,
6. die Anforderungen an die Erteilung von Auskünften über Bestands- und Nutzungsdaten durch Anbieter von digitalen Diensten,
7. den Schutz der Privatsphäre bei Endeinrichtungen hinsichtlich der Anforderungen an die Speicherung von Informationen in Endeinrichtungen der Endnutzer und den Zugriff auf Informationen, die bereits in Endeinrichtungen der Endnutzer gespeichert sind, und
8. die Aufsichtsbehörden und die Aufsicht im Hinblick auf den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation; bei digitalen Diensten bleiben die Aufsicht durch die nach Landesrecht zuständigen Behörden und § 40 des Bundesdatenschutzgesetzes unberührt.

(2) Dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, stehen den personenbezogenen Daten gleich.

(3) Diesem Gesetz unterliegen alle Unternehmen und Personen, die im Geltungsbereich dieses Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen. § 3 des Digitale-Dienste-Gesetzes bleibt unberührt.

§ 2 Begriffsbestimmungen

(1) Die Begriffsbestimmungen des Telekommunikationsgesetzes, des Digitale-Dienste-Gesetzes und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) gelten auch für dieses Gesetz, soweit in Absatz 2 keine abweichende Begriffsbestimmung getroffen wird.

(2) Im Sinne dieses Gesetzes ist oder sind

1. „Anbieter von digitalen Diensten“ jede natürliche oder juristische Person, die eigene oder fremde digitale Dienste erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden digitalen Diensten vermittelt,
2. „Bestandsdaten“ im Sinne des Teils 3 dieses Gesetzes die personenbezogenen Daten, deren Verarbeitung zum Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Anbieter von digitalen Diensten und dem Nutzer über die Nutzung von digitalen Diensten erforderlich ist,
3. „Nutzungsdaten“ die personenbezogenen Daten eines Nutzers von digitalen Diensten, deren Verarbeitung erforderlich ist, um die Inanspruchnahme von digitalen Diensten zu ermöglichen und abzurechnen; dazu gehören 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 digitalen Dienste,
4. „Nachricht“ jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen Telekommunikationsdienst ausgetauscht oder weitergeleitet wird; davon ausgenommen sind Informationen, die als Teil eines Rundfunkdienstes über ein öffentliches Telekommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Nutzer, der sie erhält, in Verbindung gebracht werden können,
5. „Dienst mit Zusatznutzen“ jeder von einem Anbieter eines Telekommunikationsdienstes bereitgehaltene zusätzliche Dienst, der die Verarbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder für die Entgeltabrechnung des Telekommunikationsdienstes erforderliche Maß hinausgeht,
6. „Endeinrichtung“ jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet.

Teil 2
Datenschutz und Schutz der Privatsphäre in der Telekommunikation

Kapitel 1
Vertraulichkeit der Kommunikation

§ 3 Vertraulichkeit der Kommunikation – 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 sind verpflichtet

1. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
2. Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
3. Betreiber öffentlicher Telekommunikationsnetze und
4. Betreiber von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden.

Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

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

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

Fußnote

(+++ § 3 Abs. 4: Zur Geltung vgl. § 5 Abs. 2 Satz 2 +++)

§ 4 Rechte des Erben des Endnutzers und anderer berechtigter Personen

Das Fernmeldegeheimnis steht der Wahrnehmung von Rechten gegenüber dem Anbieter des Telekommunikationsdienstes nicht entgegen, wenn diese Rechte statt durch den betroffenen Endnutzer durch seinen Erben oder eine andere berechtigte Person, die zur Wahrnehmung der Rechte des Endnutzers befugt ist, wahrgenommen werden.

§ 5 Abhörverbot, Geheimhaltungspflicht der Betreiber von Funkanlagen

(1) Mit einer Funkanlage (§ 3 Absatz 1 Nr 1 des Funkanlagengesetzes) dürfen nur solche Nachrichten abgehört oder in vergleichbarer Weise zur Kenntnis genommen werden, die für den Betreiber der Funkanlage, für Funkamateure im Sinne des § 2 Nummer 1 des Amateurfunkgesetzes, für die Allgemeinheit oder für einen unbestimmten Personenkreis bestimmt sind.

(2) Der Inhalt anderer als in Absatz 1 genannter Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht zur Geheimhaltung nicht schon nach § 3 besteht, anderen nicht mitgeteilt werden. § 3 Absatz 4 gilt entsprechend.

(3) Das Abhören oder die in vergleichbarer Weise erfolgende Kenntnisnahme und die Weitergabe von Nachrichten aufgrund besonderer gesetzlicher Ermächtigung bleiben unberührt.

§ 6 Nachrichtenübermittlung mit Zwischenspeicherung

(1) Nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 Verpflichtete dürfen bei Diensten, für deren Durchführung eine Zwischenspeicherung erforderlich ist, Nachrichteninhalte, insbesondere Sprach-, Ton-, Text- und Grafikmitteilungen von Endnutzern, im Rahmen eines hierauf gerichteten Diensteangebots verarbeiten, wenn

1. die Verarbeitung ausschließlich in Telekommunikationsanlagen des zwischenspeichernden Anbieters erfolgt, es sei denn, die Nachrichteninhalte werden im Auftrag des Endnutzers oder durch Eingabe des Endnutzers in Telekommunikationsanlagen anderer Anbieter weitergeleitet;
2. ausschließlich der Endnutzer
   a) durch seine Eingabe Inhalt, Umfang und Art der Verarbeitung bestimmt und
   b) bestimmt, wer Nachrichteninhalte eingeben und darauf zugreifen darf, und
3. der Verpflichtete
   a) dem Endnutzer mitteilen darf, dass der Empfänger auf die Nachricht zugegriffen hat, und
   b) Nachrichteninhalte nur entsprechend dem mit dem Endnutzer geschlossenen Vertrag löschen darf.

(2) Nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 Verpflichtete haben die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten innerhalb des Unternehmens des Anbieters und 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.

§ 7 Verlangen eines amtlichen Ausweises

(1) Anbieter und mitwirkende Personen nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 können im Zusammenhang mit dem Begründen und dem Ändern eines Vertragsverhältnisses mit einem Endnutzer über das Erbringen von Telekommunikationsdiensten die Vorlage eines amtlichen Ausweises verlangen, wenn dies zur Überprüfung der Angaben des Endnutzers erforderlich ist. Die Pflicht nach § 172 des Telekommunikationsgesetzes bleibt unberührt.

(2) Um dem Verlangen nach Vorlage eines amtlichen Ausweises zu entsprechen, kann der Endnutzer den elektronischen Identitätsnachweis gemäß § 18 des Personalausweisgesetzes, gemäß § 12 des eID-Karte-Gesetzes oder gemäß § 78 Absatz 5 des Aufenthaltsgesetzes nutzen.

(3) Von dem Ausweis darf eine Kopie erstellt werden. Die Kopie ist unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Endnutzers zu vernichten. Andere als die für den Vertragsabschluss erforderlichen Daten dürfen dabei nicht verarbeitet werden.

§ 8 Missbrauch von Telekommunikationsanlagen

(1) Es ist verboten, Telekommunikationsanlagen zu besitzen, herzustellen, auf dem Markt bereitzustellen, einzuführen oder sonst in den Geltungsbereich dieses Gesetzes zu verbringen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und aufgrund dieser Umstände oder aufgrund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen.

(2) Als zum unbemerkten Abhören oder Aufnehmen eines Bildes bestimmt gilt eine Telekommunikationsanlage insbesondere, wenn ihre Abhör- oder Aufnahmefunktion beim bestimmungsgemäßen Gebrauch des Gegenstandes für den Betroffenen nicht eindeutig erkennbar ist.

(3) Das Verbot, Telekommunikationsanlagen nach Absatz 1 zu besitzen, gilt nicht für denjenigen, der die tatsächliche Gewalt über eine solche Telekommunikationsanlage

1. als Organ, als Mitglied eines Organs, als gesetzlicher Vertreter oder als vertretungsberechtigter Gesellschafter eines Berechtigten nach Absatz 5 erlangt,
2. von einem anderen oder für einen anderen Berechtigten nach Absatz 5 erlangt, sofern und solange er die Weisungen des anderen Berechtigten über die Ausübung der tatsächlichen Gewalt über die Telekommunikationsanlage aufgrund eines Dienst-oder Arbeitsverhältnisses zu befolgen hat oder die tatsächliche Gewalt aufgrund gerichtlichen oder behördlichen Auftrags ausübt,
3. als Gerichtsvollzieher oder Vollzugsbeamter in einem Vollstreckungsverfahren erwirbt,
4. von einem Berechtigten nach Absatz 5 vorübergehend zum Zweck der sicheren Verwahrung oder der nicht gewerbsmäßigen Beförderung zu einem Berechtigten erlangt,
5. lediglich zur gewerbsmäßigen Beförderung oder gewerbsmäßigen Lagerung erlangt,
6. durch Fund erlangt, sofern er die Telekommunikationsanlage unverzüglich abliefert an den Verlierer, den Eigentümer, einen sonstigen Berechtigten nach Absatz 5 oder die für die Entgegennahme der Fundanzeige zuständige Stelle,
7. von Todes wegen erwirbt, sofern er die Telekommunikationsanlage unverzüglich einem Berechtigten nach Absatz 5 überlässt oder sie für dauernd unbrauchbar macht.

(4) Das Verbot, Telekommunikationsanlagen nach Absatz 1 zu besitzen, gilt ferner nicht für eine Telekommunikationsanlage, die durch Entfernen eines wesentlichen Bauteils dauernd unbrauchbar gemacht worden ist, sofern derjenige, der die tatsächliche Gewalt über eine solche Telekommunikationsanlage erlangt, den Erwerb unverzüglich der Bundesnetzagentur schriftlich anzeigt. Die Anzeige muss folgende Angaben enthalten:

1. Name, Vornamen und Anschrift des Erwerbers,
2. die Art der Telekommunikationsanlage, deren Hersteller- oder Warenzeichen und, wenn die Telekommunikationsanlage eine Herstellungsnummer hat, auch diese,
3. die glaubhafte Darlegung, dass der Erwerber die Telekommunikationsanlage ausschließlich zu Sammlerzwecken erworben hat.

(5) Die zuständigen obersten Bundes- oder Landesbehörden lassen Ausnahmen von Absatz 1 zu, wenn es im öffentlichen Interesse, insbesondere aus Gründen der öffentlichen Sicherheit oder zum Zweck der Lehre über oder der Forschung an entsprechenden Telekommunikationsanlagen erforderlich ist. Absatz 1 gilt ferner nicht, soweit das Bundesamt für Wirtschaft und Ausfuhrkontrolle die Ausfuhr der Telekommunikationsanlagen genehmigt hat, und nicht für technische Mittel von Behörden, die diese in den Grenzen ihrer gesetzlichen Befugnisse zur Durchführung von technischen Ermittlungsmaßnahmen einsetzen.

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

Kapitel 2
Verkehrsdaten, Standortdaten

§ 9 Verarbeitung von Verkehrsdaten

(1) Nach § 3 Absatz 2 Satz 1 Verpflichtete dürfen folgende Verkehrsdaten nur verarbeiten, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen und

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

Im Übrigen sind Verkehrsdaten von den nach § 3 Absatz 2 Satz 1 Verpflichteten nach Beendigung der Verbindung unverzüglich zu löschen. Eine über Satz 1 hinausgehende Verarbeitung der Verkehrsdaten ist unzulässig. Die Pflicht zur Verarbeitung von Verkehrsdaten aufgrund von anderen Rechtsvorschriften bleibt unberührt.

(2) Teilnehmerbezogene Verkehrsdaten nach Absatz 1 dürfen vom Anbieter des Telekommunikationsdienstes zum Zweck der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und im dazu erforderlichen Zeitraum nur verwendet werden, wenn der Endnutzer in diese Verwendung gemäß der Verordnung (EU) 2016/679 eingewilligt hat. Die Daten anderer Endnutzer sind unverzüglich zu anonymisieren. Eine zielnummernbezogene Verwendung der Verkehrsdaten zu den in Satz 1 genannten Zwecken ist nur zulässig, wenn der Endnutzer gemäß der Verordnung (EU) 2016/679 informiert wurde und er eingewilligt hat. Hierbei sind die Daten anderer Endnutzer unverzüglich zu anonymisieren. Außerdem ist der Endnutzer darauf hinzuweisen, dass er die Einwilligung nach den Sätzen 1 und 3 jederzeit widerrufen kann.

§ 10 Entgeltermittlung und Entgeltabrechnung

(1) Die Verarbeitung der Verkehrsdaten nach § 9 Absatz 1 Satz 1 durch nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 Verpflichtete zur Ermittlung des Entgelts und zur Abrechnung mit den Endnutzern darf nur nach Maßgabe der Absätze 2 bis 4 erfolgen. Erbringt ein Anbieter eines Telekommunikationsdienstes seine Dienste über ein öffentliches Telekommunikationsnetz eines anderen Betreibers, darf dieser Betreiber dem Anbieter des Telekommunikationsdienstes die für die Erbringung von dessen Diensten erhobenen Verkehrsdaten übermitteln. Hat der Anbieter eines Telekommunikationsdienstes mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er dem Dritten die Verkehrsdaten nach § 9 Absatz 1 Satz 1 Nummer 1 bis 3 und 5 nur übermitteln, soweit es zum Einzug des Entgelts und der Erstellung einer detaillierten Rechnung erforderlich ist. Der Dritte darf die Daten nur zu diesem Zweck verarbeiten. Der Dritte ist vertraglich zur Wahrung des Fernmeldegeheimnisses und des dem Anbieter des Telekommunikationsdienstes obliegenden Datenschutzes zu verpflichten.

(2) Nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 Verpflichtete haben nach Beendigung der Verbindung aus den Verkehrsdaten nach § 9 Absatz 1 Satz 1 Nummer 1 bis 3 und 5 unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen. Hat der Endnutzer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

(3) Soweit es für die Abrechnung des Anbieters eines Telekommunikationsdienstes mit anderen Anbietern von Telekommunikationsdiensten oder mit deren Endnutzern sowie für die Abrechnung anderer Anbieter mit ihren Endnutzern erforderlich ist, dürfen der Anbieter und mitwirkende Personen nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 die für die Berechnung des Entgelts erforderlichen Verkehrsdaten nach § 9 Absatz 1 Satz 1 Nummer 1 bis 3 und 5 verarbeiten.

(4) Ziehen der Anbieter und mitwirkende Personen nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 mit der Rechnung Entgelte für Leistungen eines Dritten ein, die dieser im Zusammenhang mit der Erbringung von Telekommunikationsdiensten erbracht hat, so dürfen dem Dritten Verkehrsdaten nach § 9 Absatz 1 Satz 1 Nummer 1 bis 3 und 5 übermittelt werden, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Endnutzer erforderlich sind.

§ 11 Einzelverbindungsnachweis

(1) Dem Endnutzer sind die Verkehrsdaten nach § 9 Absatz 1 Satz 1 Nummer 1 bis 3 derjenigen Verbindungen, für die er entgeltpflichtig ist, durch Anbieter und mitwirkende Personen nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 mitzuteilen, wenn er vor dem maßgeblichen Abrechnungszeitraum einen Einzelverbindungsnachweis verlangt hat. Auf Wunsch dürfen ihm auch die Daten pauschal abgegoltener Verbindungen mitgeteilt werden. Dabei entscheidet der Endnutzer, ob ihm die von ihm gewählten Rufnummern ungekürzt oder unter Kürzung um die letzten drei Ziffern mitgeteilt werden. Bei einem Teilnehmeranschluss im Haushalt ist die Mitteilung nur zulässig, wenn der Anschlussinhaber in Textform erklärt hat, dass er alle zum Haushalt gehörenden Personen, die den Teilnehmeranschluss nutzen, darüber informiert hat und künftige Mitnutzer des Teilnehmeranschlusses unverzüglich darüber informieren wird, dass dem Inhaber des Teilnehmeranschlusses die Verkehrsdaten nach Satz 1 zur Erteilung des Einzelverbindungsnachweises bekannt gegeben werden.

(2) Unbeschadet des Absatzes 1 dürfen dem Endnutzer die Verkehrsdaten nach Absatz 1 Satz 1 mitgeteilt werden, wenn er Einwendungen gegen die Höhe der Verbindungsentgelte erhoben hat. Das gilt auch für einen Mobilfunkanschluss.

(3) Bei Teilnehmeranschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Inhaber des Teilnehmeranschlusses in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. Soweit die öffentlich-rechtlichen Religionsgesellschaften für ihren Bereich eigene Mitarbeitervertreterregelungen erlassen haben, findet Satz 1 mit der Maßgabe Anwendung, dass an die Stelle des Betriebsrates oder der Personalvertretung die jeweilige Mitarbeitervertretung tritt.

(4) Soweit ein Anschlussinhaber zur vollständigen oder teilweisen Übernahme der Entgelte für Verbindungen verpflichtet ist, die bei seinem Anschluss ankommen, dürfen ihm in dem für ihn bestimmten Einzelverbindungsnachweis die Nummern der Anschlüsse, von denen die Anrufe ausgingen, nur unter Kürzung um die letzten drei Ziffern mitgeteilt werden.

(5) Der Einzelverbindungsnachweis nach Absatz 1 Satz 1 darf nicht Verbindungen zu Anschlüssen erkennen lassen,

1. deren Inhaber Personen, Behörden oder Organisationen in sozialen oder kirchlichen Bereichen sind, die grundsätzlich anonym bleibenden Endnutzern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verpflichtungen zur Verschwiegenheit unterliegen, und
2. die die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) in eine Liste aufgenommen hat.

(6) Der Beratung im Sinne des Absatzes 5 Nummer 1 dienen neben den in § 203 Absatz 1 Nummer 4 und 5 des Strafgesetzbuches genannten Personengruppen insbesondere die Telefonseelsorge und die Gesundheitsberatung. Die Bundesnetzagentur nimmt die Inhaber der Anschlüsse auf Antrag in die Liste auf, wenn sie die Aufgabenbestimmung nach Absatz 5 Nummer 1 durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts nachgewiesen haben. Die Liste wird zum Abruf im automatisierten Verfahren bereitgestellt. Die Verpflichteten nach § 3 Absatz 2 Satz 1, die Einzelverbindungsnachweise erstellen, haben die Liste quartalsweise abzufragen und Änderungen unverzüglich in ihren Abrechnungsverfahren anzuwenden.

§ 12 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) Soweit erforderlich, dürfen Verpflichtete nach § 3 Absatz 2 Satz 1 Verkehrsdaten der Endnutzer sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, verarbeiten, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Telekommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Eine Verarbeitung der Verkehrsdaten und Steuerdaten zu anderen Zwecken ist unzulässig. Soweit die Verkehrsdaten nicht automatisiert erhoben und verwendet werden, muss der Datenschutzbeauftragte des Verpflichteten nach § 3 Absatz 2 Satz 1 unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden. Betroffene Endnutzer sind von dem nach § 3 Absatz 2 Satz 1 Verpflichteten zu benachrichtigen, sofern sie ermittelt werden können.

(2) Die Verkehrsdaten und Steuerdaten sind unverzüglich zu löschen, sobald sie für die Beseitigung der Störung nicht mehr erforderlich sind.

(3) Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber von Telekommunikationsnetzen oder seinem Beauftragten das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist. Eventuelle bei der Aufschaltung erstellte Aufzeichnungen sind unverzüglich zu löschen. Das Aufschalten muss den betroffenen Kommunikationsteilnehmern durch ein akustisches oder sonstiges Signal zeitgleich angezeigt und ausdrücklich mitgeteilt werden. Sofern dies technisch nicht möglich ist, muss der betriebliche Datenschutzbeauftragte des Betreibers des Telekommunikationsnetzes unverzüglich detailliert über die Verfahren und Umstände der

Maßnahme informiert werden. Diese Informationen hat der betriebliche Datenschutzbeauftragte für zwei Jahre aufzubewahren.

(4) Wenn tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme eines Telekommunikationsnetzes oder Telekommunikationsdienstes vorliegen, insbesondere für eine Leistungserschleichung oder einen Betrug oder eine unzumutbare Belästigung nach § 7 des Gesetzes gegen den unlauteren Wettbewerb, darf der Verpflichtete nach § 3 Absatz 2 Satz 1 zur Sicherung seines Entgeltanspruchs sowie zum Schutz der Endnutzer vor der rechtswidrigen Inanspruchnahme des Telekommunikationsdienstes oder des Telekommunikationsnetzes Verkehrsdaten verarbeiten, die erforderlich sind, um die rechtswidrige Inanspruchnahme des Telekommunikationsnetzes oder Telekommunikationsdienstes aufzudecken und zu unterbinden. Die Anhaltspunkte für die rechtwidrige Inanspruchnahme des Telekommunikationsnetzes oder Telekommunikationsdienstes hat der nach § 3 Absatz 2 Satz 1 Verpflichtete zu dokumentieren. Der nach § 3 Absatz 2 Satz 1 Verpflichtete darf aus den Verkehrsdaten nach Satz 1 einen pseudonymisierten Gesamtdatenbestand bilden, der Aufschluss über die von einzelnen Endnutzern erzielten Umsätze gibt und unter Zugrundelegung geeigneter Kriterien das Auffinden solcher Verbindungen des Netzes ermöglicht, bei denen der Verdacht einer rechtswidrigen Inanspruchnahme besteht. Die Verkehrsdaten anderer Verbindungen sind unverzüglich zu löschen. Die Aufsichtsbehörde ist über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.

§ 13 Standortdaten

(1) Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten verarbeitet werden, dürfen nur in dem zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Nutzer vom Anbieter des Dienstes mit Zusatznutzen gemäß der Verordnung (EU) 2016/679 informiert wurde und eingewilligt hat. Der Anbieter des Dienstes mit Zusatznutzen hat bei jeder Feststellung des Standortes des Mobilfunkendgerätes den Endnutzer durch eine Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurden, über die Feststellung des Standortes zu informieren. Dies gilt nicht, wenn der Standort nur auf dem Endgerät angezeigt wird, dessen Standortdaten ermittelt wurden. Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Nutzer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Nutzer seine Einwilligung ausdrücklich, gesondert und schriftlich gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilen. In diesem Fall gilt die Verpflichtung nach Satz 2 entsprechend für den Anbieter des Dienstes mit Zusatznutzen. Der Anschlussinhaber muss weitere Nutzer seines Mobilfunkanschlusses über eine erteilte Einwilligung unterrichten.

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

(3) Bei Verbindungen zu Anschlüssen, die unter den Notrufnummern 112 oder 110 oder den Rufnummern 124 124 oder 116 117 erreicht werden, haben der Anbieter und mitwirkende Personen nach § 3 Absatz 2 Satz 1 Nummer 1 und 2 sicherzustellen, dass nicht im Einzelfall oder dauernd die Übermittlung von Standortdaten ausgeschlossen wird.

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

Kapitel 3
Mitteilen ankommender Verbindungen, Rufnummernanzeige und -unterdrückung, automatische Anrufweiterschaltung

§ 14 Mitteilen ankommender Verbindungen

(1) Trägt ein Anschlussinhaber in einem Verfahren schlüssig vor, dass bei seinem Anschluss bedrohende oder belästigende Anrufe ankommen, hat der Anbieter des Telekommunikationsdienstes auf schriftlichen Antrag auch netzübergreifend Auskunft über die Inhaber der Anschlusskennungen zu erteilen, von denen die Verbindungen ausgehen; das Verfahren ist zu dokumentieren. Die Auskunft darf sich nur auf Verbindungen und Verbindungsversuche beziehen, die nach Stellung des Antrags stattgefunden haben. Der Anbieter des Telekommunikationsdienstes darf die Anschlusskennungen, Namen und Anschriften der Inhaber dieser

Anschlusskennungen sowie Datum und Uhrzeit des Beginns der Verbindungen und der Verbindungsversuche verarbeiten sowie diese Daten dem betroffenen Anschlussinhaber mitteilen.

(2) Die Bekanntgabe nach Absatz 1 Satz 3 darf nur erfolgen, wenn der betroffene Anschlussinhaber des betroffenen Anschlusses zuvor die Verbindungen nach Datum, Uhrzeit oder anderen geeigneten Kriterien eingrenzt, soweit ein Missbrauch dieses Verfahrens nicht auf andere Weise ausgeschlossen werden kann.

(3) Im Fall einer netzübergreifenden Auskunft sind die an der Verbindung mitwirkenden anderen Anbieter und Betreiber nach § 3 Absatz 2 Satz 1 verpflichtet, dem Anbieter des Telekommunikationsdienstes des bedrohten oder belästigten Anschlussinhabers die erforderlichen Auskünfte zu erteilen, sofern sie über diese Daten verfügen.

(4) Der Inhaber der Anschlusskennung, von der die festgestellten Verbindungen ausgegangen sind, ist darüber zu unterrichten, dass über diese Verbindungen Auskunft erteilt wurde. Davon kann abgesehen werden, wenn der Antragsteller schriftlich schlüssig vorgetragen hat, dass ihm aus dieser Mitteilung wesentliche Nachteile entstehen können, und diese Nachteile bei Abwägung mit den schutzwürdigen Interessen der Anrufenden als wesentlich schwerwiegender erscheinen. Erhält der Inhaber der Anschlusskennung, von der die als bedrohend oder belästigend bezeichneten Anrufe ausgegangen sind, auf andere Weise Kenntnis von der Auskunftserteilung nach Absatz 1 Satz 3, so ist er auf Verlangen über die Auskunftserteilung zu unterrichten.

(5) Die Aufsichtsbehörde ist über die Einführung und Änderungen des Verfahrens zur Einhaltung der Anforderungen der Absätze 1 bis 4 unverzüglich in Kenntnis zu setzen.

§ 15 Rufnummernanzeige und -unterdrückung

(1) Bietet der Anbieter eines Sprachkommunikationsdienstes bei Anrufen die Anzeige der Rufnummer der anrufenden Endnutzer an, so müssen anrufende und angerufene Endnutzer die Möglichkeit haben, die Rufnummernanzeige dauernd oder für jeden Anruf einzeln auf einfache Weise und unentgeltlich zu unterdrücken. Angerufene Endnutzer müssen die Möglichkeit haben, eingehende Anrufe, bei denen die Rufnummernanzeige durch den anrufenden Endnutzer unterdrückt wurde, auf einfache Weise und unentgeltlich abzuweisen. Wird die Anzeige der Rufnummer von angerufenen Endnutzern angeboten, so müssen angerufene Endnutzer die Möglichkeit haben, die Anzeige ihrer Rufnummer beim anrufenden Endnutzer auf einfache Weise und unentgeltlich zu unterdrücken. Die Anzeige von Rufnummern von anrufenden Endnutzern darf bei den Notrufnummern 112 und 110 sowie den Rufnummern 124 124 und 116 117 nicht ausgeschlossen werden.

(2) Bei Anrufen zum Zweck der Werbung dürfen anrufende Nutzer weder die Rufnummernanzeige unterdrücken noch bei dem Anbieter des Telekommunikationsdienstes veranlassen, dass diese unterdrückt wird; der anrufende Nutzer hat sicherzustellen, dass dem Angerufenen die dem anrufenden Nutzer zugeteilte Rufnummer übermittelt wird.

(3) Sofern Anschlussinhaber es beantragen, müssen Anbieter von Sprachkommunikationsdiensten einen Anschluss bereitstellen, bei dem die Übermittlung der Rufnummer unentgeltlich ausgeschlossen ist. Auf Antrag des Anschlussinhabers sind solche Anschlüsse im Endnutzerverzeichnis (§ 17) zu kennzeichnen. Ist eine Kennzeichnung nach Satz 2 erfolgt, so darf an den gekennzeichneten Anschluss eine Übermittlung der Rufnummer des Anschlusses, von dem der Anruf ausgeht, erst dann erfolgen, wenn die Kennzeichnung in der aktualisierten Fassung des Endnutzerverzeichnisses nicht mehr enthalten ist.

(4) Hat der Anschlussinhaber die Eintragung in das Endnutzerverzeichnis nicht nach § 17 beantragt, unterbleibt die Anzeige seiner Rufnummer bei dem angerufenen Anschluss, es sei denn, dass der Anschlussinhaber die Übermittlung seiner Rufnummer ausdrücklich wünscht.

(5) Die Absätze 1 bis 4 gelten auch für Anrufe in das Ausland und für aus dem Ausland kommende Anrufe, soweit sie Anrufende oder Angerufene im Inland betreffen.

§ 16 Automatische Anrufweiterschaltung

Anbieter von Sprachkommunikationsdiensten sind verpflichtet, ihren Endnutzern die Möglichkeit einzuräumen, eine von einem Dritten veranlasste automatische Weiterschaltung auf das Endgerät des Endnutzers auf einfache Weise und unentgeltlich abzustellen, soweit dies technisch möglich ist.

Kapitel 4
Endnutzerverzeichnisse, Bereitstellen von Endnutzerdaten

§ 17 Endnutzerverzeichnisse

(1) Anschlussinhaber können mit ihrer Rufnummer, ihrem Namen und ihrer Anschrift in gedruckte oder elektronische Endnutzerverzeichnisse, die der Öffentlichkeit unmittelbar oder über Auskunftsdienste zugänglich sind, eingetragen werden, soweit sie dies beantragen. Vor ihrem Antrag sind die Anschlussinhaber über weitere Nutzungsmöglichkeiten aufgrund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren. Auf Antrag können zusätzliche Angaben wie Beruf und Branche eingetragen werden. Dabei können die Antragsteller bestimmen, welche Angaben in den Verzeichnissen veröffentlicht werden sollen. Auf Verlangen des Antragstellers dürfen weitere Nutzer des Anschlusses mit Namen und Vornamen eingetragen werden, soweit diese damit einverstanden sind. Für die Einträge nach Satz 1 darf ein Entgelt nicht erhoben werden.

(2) Der Anbieter eines nummerngebundenen interpersonellen Telekommunikationsdienstes hat Anschlussinhaber bei der Begründung des Vertragsverhältnisses über die Möglichkeit zu informieren, ihre Rufnummer, ihren Namen, ihren Vornamen und ihre Anschrift in Endnutzerverzeichnisse nach Absatz 1 Satz 1 aufzunehmen.

(3) Der Anschlussinhaber kann von seinem Anbieter des nummerngebundenen interpersonellen Telekommunikationsdienstes jederzeit verlangen, dass seine Rufnummer, sein Name, sein Vorname und seine Anschrift in Auskunfts- und Verzeichnismedien unentgeltlich eingetragen, gespeichert, berichtigt oder gelöscht werden.

(4) Anbieter von Auskunfts- und Verzeichnismedien sind verpflichtet, die gemäß § 18 Absatz 1 übermittelten Daten zu veröffentlichen sowie unrichtige oder gelöschte Daten aus den Verzeichnissen zu entfernen und Berichtigungen vorzunehmen.

§ 18 Bereitstellen von Endnutzerdaten

(1) Jeder Anbieter eines nummerngebundenen interpersonellen Telekommunikationsdienstes hat unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen jedem Unternehmen Endnutzerdaten nach § 17 Absatz 1 auf Antrag zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten, Diensten zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers und von Endnutzerverzeichnissen bereitzustellen.

(2) Für die Bereitstellung der Daten kann ein Entgelt verlangt werden. Das Entgelt unterliegt in der Regel einer nachträglichen Missbrauchsprüfung durch die Bundesnetzagentur nach Maßgabe der Bestimmungen des Telekommunikationsgesetzes zur Missbrauchsprüfung von Entgelten. Ein Entgelt kann nur dann der Entgeltgenehmigungspflicht nach dem Telekommunikationsgesetz unterworfen werden, wenn das Unternehmen, von dem die Endnutzerdaten bereitgestellt werden, auf dem Markt für Endnutzerdaten über eine beträchtliche Marktmacht verfügt.

(3) Die Bereitstellung der Daten nach Absatz 1 hat unverzüglich nach einem Antrag nach Absatz 1 und in nichtdiskriminierender Weise zu erfolgen.

(4) Die nach Absatz 1 bereitgestellten Daten müssen vollständig sein und inhaltlich sowie technisch so aufbereitet sein, dass sie nach dem jeweiligen Stand der Technik ohne Schwierigkeiten in ein kundenfreundlich gestaltetes Endnutzerverzeichnis oder in eine entsprechende Auskunftsdienste-Datenbank aufgenommen werden können.

Teil 3
Datenschutz bei digitalen Diensten, Endeinrichtungen

Kapitel 1
Technische und organisatorische Vorkehrungen, Verarbeitung von Daten zum Zweck des Jugendschutzes und zur Auskunftserteilung

§ 19 Technische und organisatorische Vorkehrungen

(1) Anbieter von digitalen Diensten haben durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer von digitalen Diensten

1. die Nutzung des Dienstes jederzeit beenden kann und
2. digitale Dienste geschützt gegen Kenntnisnahme Dritter in Anspruch nehmen kann.

(2) Anbieter von digitalen Diensten haben die Nutzung von digitalen Diensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer von digitalen Diensten ist über diese Möglichkeit zu informieren.

(3) Die Weitervermittlung zu einem anderen Anbieter von digitalen Diensten ist dem Nutzer anzuzeigen.

(4) Anbieter von digitalen Diensten haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene digitale Dienste durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die technischen Einrichtungen, die sie für das Angebot ihrer digitalen Dienste nutzen, möglich ist und
2. die technischen Einrichtungen nach Nummer 1 gesichert sind gegen Störungen, auch gegen solche, die durch äußere Angriffe bedingt sind.

Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Vorkehrung nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens. Anordnungen des Bundesamtes für Sicherheit in der Informationstechnik nach § 7d Satz 1 BSI-Gesetz bleiben unberührt.

§ 20 Verarbeitung personenbezogener Daten Minderjähriger

Hat ein Anbieter von digitalen Diensten zur Wahrung des Jugendschutzes personenbezogene Daten von Minderjährigen erhoben, etwa durch Mittel zur Altersverifikation oder andere technische Maßnahmen, oder anderweitig gewonnen, so darf er diese Daten nicht für kommerzielle Zwecke verarbeiten.

§ 21 Bestandsdaten

(1) Auf Anordnung der zuständigen Stellen dürfen Anbieter von digitalen Diensten im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

(2) Der Anbieter von digitalen Diensten darf darüber hinaus im Einzelfall Auskunft über bei ihm vorhandene Bestandsdaten erteilen, soweit dies zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger audiovisueller Inhalte oder aufgrund von Inhalten, die den Tatbestand der §§ 86, 86a, 89a, 91, 100a, 111, 126, 129 bis 129b, 130, 131, 140, 166, 184b, 185 bis 187, 189, 201a, 241 oder 269 des Strafgesetzbuches erfüllen und nicht gerechtfertigt sind, erforderlich ist.

(3) Für die Erteilung der Auskunft nach Absatz 2 ist eine vorherige gerichtliche Anordnung über die Zulässigkeit der Auskunftserteilung erforderlich, die vom Verletzten zu beantragen ist. Das Gericht entscheidet zugleich über die Verpflichtung zur Auskunftserteilung, sofern der Antrag nicht ausdrücklich auf die Anordnung der Zulässigkeit der Auskunftserteilung beschränkt ist. Für den Erlass dieser Anordnung ist das Landgericht ohne Rücksicht auf den Streitwert zuständig. Örtlich zuständig ist das Gericht, in dessen Bezirk der Verletzte seinen Wohnsitz, seinen Sitz oder eine Niederlassung hat. Die Entscheidung trifft die Zivilkammer. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die Kosten der richterlichen Anordnung trägt der Verletzte. Gegen die Entscheidung des Landgerichts ist die Beschwerde statthaft.

(4) Der Anbieter von digitalen Diensten ist als Beteiligter zu dem Verfahren nach Absatz 3 hinzuzuziehen. Er darf den Nutzer über die Einleitung des Verfahrens unterrichten.

§ 22 Auskunftsverfahren bei Bestandsdaten

(1) Wer geschäftsmäßig digitale Dienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, darf die Bestandsdaten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt nicht für Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Bestandsdaten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Nutzungsdaten auch automatisiert ausgewertet werden. Für die Auskunftserteilung sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) Die Auskunft darf nur erteilt werden nach Maßgabe der nachfolgenden Absätze und soweit die um die Auskunft ersuchende Stelle dies im Einzelfall unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr

eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt. Das Auskunftsverlangen ist schriftlich oder elektronisch zu stellen. Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich schriftlich oder elektronisch zu bestätigen. Die Verantwortung für die Zulässigkeit der Auskunft tragen die um Auskunft ersuchenden Stellen.

(3) Die Auskunft nach Absatz 1 Satz 1 darf nur erteilt werden an

1. die für die Verfolgung von Straftaten und Ordnungswidrigkeiten zuständigen Behörden, soweit zureichende tatsächliche Anhaltspunkte für eine Straftat oder Ordnungswidrigkeit, die gegenüber einer natürlichen Person mit Geldbuße im Höchstmaß von mehr als fünfzehntausend Euro bedroht ist, vorliegen und die in die Auskunft aufzunehmenden Daten erforderlich sind, um den Sachverhalt zu erforschen, den Aufenthaltsort eines Beschuldigten oder Betroffenen zu ermitteln oder eine Strafe zu vollstrecken,
2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden, soweit die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind,
   a) zur Abwehr einer Gefahr für die öffentliche Sicherheit, oder
   b) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung, Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie nicht unerheblichen Sachwerten, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes sowie zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder
   c) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung sowie Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in einem übersehbaren Zeitraum eine gegen ein solches Rechtsgut gerichtete Straftat begehen wird, oder
   d) zur Verhütung einer Straftat von erheblicher Bedeutung, sofern Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine ihrer Art nach konkretisierte Weise als Täter oder Teilnehmer an der Begehung einer Tat beteiligt ist, oder
   e) zur Verhütung einer schweren Straftat im Sinne von § 100a Absatz 2 der Strafprozessordnung, sofern das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass die Person innerhalb eines übersehbaren Zeitraums die Tat begehen wird,
3. das Bundeskriminalamt als Zentralstelle nach § 2 des Bundeskriminalamtgesetzes, sofern
   a) zureichende tatsächliche Anhaltspunkte für eine Straftat im Sinne des § 2 Absatz 1 des Bundeskriminalamtgesetzes vorliegen und die in die Auskunft aufzunehmenden Daten erforderlich sind, um
      aa) die zuständige Strafverfolgungsbehörde zu ermitteln oder
      bb) ein Auskunftsersuchen einer ausländischen Strafverfolgungsbehörde im Rahmen des internationalen polizeilichen Dienstverkehrs, das nach Maßgabe der Vorschriften über die internationale Rechtshilfe in Strafsachen bearbeitet wird, zu erledigen, oder
   b) die in die Auskunft aufzunehmenden Daten im Rahmen der Strafvollstreckung erforderlich sind, um ein Auskunftsersuchen einer ausländischen Strafverfolgungsbehörde im Rahmen des polizeilichen Dienstverkehrs, das nach Maßgabe der Vorschriften über die internationale Rechtshilfe in Strafsachen bearbeitet wird, zu erledigen, oder
   c) die Gefahr besteht, dass eine Person an der Begehung einer Straftat im Sinne des § 2 Absatz 1 des Bundeskriminalamtgesetzes beteiligt sein wird, und die in die Auskunft aufzunehmenden Daten erforderlich sind, um
      aa) die für die Verhütung der Straftat zuständige Polizeibehörde zu ermitteln oder
      bb) ein Auskunftsersuchen einer ausländischen Polizeibehörde im Rahmen des polizeilichen Dienstverkehrs zur Verhütung der Straftat zu erledigen, oder
   d) Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise an einer Straftat von erheblicher Bedeutung beteiligt sein wird und die in die Auskunft aufzunehmenden Daten erforderlich sind, um

aa) die für die Verhütung der Straftat zuständige Polizeibehörde zu ermitteln oder

bb) ein Auskunftsersuchen einer ausländischen Polizeibehörde im Rahmen des polizeilichen Dienstverkehrs zur Verhütung der Straftat zu erledigen, oder

e) das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine schwere Straftat nach § 100a Absatz 2 der Strafprozessordnung begehen wird, und die in die Auskunft aufzunehmenden Daten erforderlich sind, um

aa) die für die Verhütung der Straftat zuständige Polizeibehörde zu ermitteln oder

bb) ein Auskunftsersuchen einer ausländischen Polizeibehörde im Rahmen des polizeilichen Dienstverkehrs zur Verhütung der Straftat zu erledigen,

4. das Zollkriminalamt als Zentralstelle nach § 3 des Zollfahndungsdienstgesetzes, sofern

a) im Einzelfall zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen und die in die Auskunft aufzunehmenden Daten erforderlich sind, um

aa) die zuständige Strafverfolgungsbehörde zu ermitteln oder

bb) ein Auskunftsersuchen einer ausländischen Strafverfolgungsbehörde im Rahmen des internationalen polizeilichen Dienstverkehrs, das nach Maßgabe der Vorschriften über die internationale Rechtshilfe in Strafsachen bearbeitet wird, auch im Rahmen der Strafvollstreckung, zu erledigen, oder

b) dies im Einzelfall erforderlich ist

aa) zur Abwehr einer Gefahr für die öffentliche Sicherheit, oder

bb) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung, Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie nicht unerheblichen Sachwerten, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder

cc) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung sowie Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass die Gefährdung eines solchen Rechtsgutes in einem übersehbaren Zeitraum eintreten wird, oder

dd) zur Erledigung eines Auskunftsersuchens einer ausländischen Polizeibehörde im Rahmen des polizeilichen Dienstverkehrs zur Verhütung einer Straftat, oder

ee) zur Verhütung einer Straftat von erheblicher Bedeutung, sofern Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine ihrer Art nach konkretisierte Weise als Täter oder Teilnehmer an der Begehung der Tat beteiligt ist, oder

ff) zur Verhütung einer schweren Straftat nach § 100a Absatz 2 der Strafprozessordnung, sofern das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass die Person innerhalb eines übersehbaren Zeitraums die Tat begehen wird,

5. die Behörden der Zollverwaltung und die nach Landesrecht zuständigen Behörden, sofern im Einzelfall bei der Veröffentlichung von Angeboten oder Werbemaßnahmen ohne Angabe von Name und Anschrift tatsächliche Anhaltspunkte für Schwarzarbeit oder illegale Beschäftigung nach § 1 des Schwarzarbeitsbekämpfungsgesetzes vorliegen und die in die Auskunft aufzunehmenden Daten zur Identifizierung des Auftraggebers erforderlich sind, um Schwarzarbeit oder illegale Beschäftigung aufzudecken,

6. die Verfassungsschutzbehörden des Bundes und der Länder, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach

a) § 3 Absatz 1 des Bundesverfassungsschutzgesetzes oder

b) einem zum Verfassungsschutz (§ 1 Absatz 1 des Bundesverfassungsschutzgesetzes) landesgesetzlich begründeten Beobachtungsauftrag der Landesbehörde, insbesondere zum Schutz der verfassungsmäßigen Ordnung vor Bestrebungen und Tätigkeiten der organisierten Kriminalität,

7. den Militärischen Abschirmdienst, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach § 1 Absatz 1 des MAD-Gesetzes oder zur Sicherung der Einsatzbereitschaft der Truppe oder zum Schutz der Angehörigen, der Dienststellen und Einrichtungen des Geschäftsbereichs des Bundesministeriums der Verteidigung nach § 14 Absatz 1 des MAD-Gesetzes erforderlich ist,

8. den Bundesnachrichtendienst, soweit dies erforderlich ist

a) zur politischen Unterrichtung der Bundesregierung, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Auskunft Informationen über das Ausland gewonnen werden können, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind und zu deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat, oder

b) zur Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Auskunft Erkenntnisse gewonnen werden können mit Bezug zu den in § 4 Absatz 3 Nummer 1 des BND-Gesetzes genannten Gefahrenbereichen oder zum Schutz der in § 4 Absatz 3 Nummer 2 und 3 des BND-Gesetzes genannten Rechtsgüter.

(4) Die Auskunft nach Absatz 1 Satz 3 darf nur erteilt werden an

1. die für die Verfolgung von Straftaten zuständigen Behörden, soweit zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen und die in die Auskunft aufzunehmenden Daten erforderlich sind, um den Sachverhalt zu erforschen, den Aufenthaltsort eines Beschuldigten zu ermitteln oder eine Strafe zu vollstrecken,

2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden, wenn die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind

a) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung, Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie nicht unerheblicher Sachwerte oder zur Verhütung einer Straftat oder

b) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung sowie Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie nicht unerheblicher Sachwerte, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes sowie zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder

c) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung sowie Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in einem übersehbaren Zeitraum eine gegen ein solches Rechtsgut gerichtete Straftat begehen wird, oder

d) zur Verhütung einer schweren Straftat nach § 100a Absatz 2 der Strafprozessordnung, sofern Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine ihrer Art nach konkretisierten Weise als Täter oder Teilnehmer an der Begehung einer Tat beteiligt ist, oder

e) zur Verhütung einer schweren Straftat nach § 100a Absatz 2 der Strafprozessordnung, sofern das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass die Person innerhalb eines übersehbaren Zeitraums die Tat begehen wird,

3. das Bundeskriminalamt als Zentralstelle nach § 2 des Bundeskriminalamtgesetzes, sofern

a) zureichende tatsächliche Anhaltspunkte für eine Straftat im Sinne des § 2 Absatz 1 des Bundeskriminalamtgesetzes vorliegen und die in die Auskunft aufzunehmenden Daten erforderlich sind, um

aa) die zuständige Strafverfolgungsbehörde zu ermitteln, oder

bb) ein Auskunftsersuchen einer ausländischen Strafverfolgungsbehörde im Rahmen des internationalen polizeilichen Dienstverkehrs, das nach Maßgabe der Vorschriften über die internationale Rechtshilfe in Strafsachen bearbeitet wird, zu erledigen, oder

b) die in die Auskunft aufzunehmenden Daten im Rahmen der Strafvollstreckung erforderlich sind, um ein Auskunftsersuchen einer ausländischen Strafverfolgungsbehörde im Rahmen des polizeilichen Dienstverkehrs, das nach Maßgabe der Vorschriften über die internationale Rechtshilfe in Strafsachen bearbeitet wird, zu erledigen,

c) die Gefahr besteht, dass eine Person an der Begehung einer Straftat im Sinne des § 2 Absatz 1 des Bundeskriminalamtgesetzes beteiligt sein wird und die in die Auskunft aufzunehmenden Daten erforderlich sind, um

aa) die für die Verhütung der Straftat zuständige Polizeibehörde zu ermitteln, oder

bb) ein Auskunftsersuchen einer ausländischen Polizeibehörde im Rahmen des polizeilichen Dienstverkehrs zur Verhütung der Straftat zu erledigen, oder

d) Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise an einer schweren Straftat nach § 100a Absatz 2 der Strafprozessordnung beteiligt sein wird, und die in die Auskunft aufzunehmenden Daten erforderlich sind, um

aa) die für die Verhütung der Straftat zuständige Polizeibehörde zu ermitteln, oder

bb) ein Auskunftsersuchen einer ausländischen Polizeibehörde im Rahmen des polizeilichen Dienstverkehrs zur Verhütung der Straftat zu erledigen, oder

e) das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine schwere Straftat nach § 100a Absatz 2 der Strafprozessordnung begehen wird, und die in die Auskunft aufzunehmenden Daten erforderlich sind, um

aa) die für die Verhütung der Straftat zuständige Polizeibehörde zu ermitteln, oder

bb) ein Auskunftsersuchen einer ausländischen Polizeibehörde im Rahmen des polizeilichen Dienstverkehrs zur Verhütung der Straftat zu erledigen,

4. das Zollkriminalamt als Zentralstelle nach § 3 des Zollfahndungsdienstgesetzes, sofern

a) im Einzelfall zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen, und die in die Auskunft aufzunehmenden Daten erforderlich sind, um

aa) die zuständige Strafverfolgungsbehörde zu ermitteln, oder

bb) ein Auskunftsersuchen einer ausländischen Strafverfolgungsbehörde im Rahmen des internationalen polizeilichen Dienstverkehrs, das nach Maßgabe der Vorschriften über die internationale Rechtshilfe in Strafsachen bearbeitet wird, auch im Rahmen der Strafvollstreckung, zu erledigen, oder

b) dies im Einzelfall erforderlich ist

aa) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung, Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie nicht unerheblicher Sachwerte oder zur Verhütung einer Straftat, oder

bb) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung sowie Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, wenn Tatsachen den Schluss auf ein wenigstens seiner

Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder

cc) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung sowie Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass die Gefährdung eines solchen Rechtsgutes in einem übersehbaren Zeitraum eintreten wird, oder

dd) zur Erledigung eines Auskunftsersuchens einer ausländischen Polizeibehörde im Rahmen des polizeilichen Dienstverkehrs zur Verhütung einer schweren Straftat nach § 100a Absatz 2 der Strafprozessordnung, oder

ee) zur Verhütung einer schweren Straftat nach § 100a Absatz 2 der Strafprozessordnung, sofern Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine ihrer Art nach konkretisierte Weise als Täter oder Teilnehmer an der Begehung der Tat beteiligt ist, oder

ff) zur Verhütung einer schweren Straftat nach § 100a Absatz 2 der Strafprozessordnung, sofern das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass die Person innerhalb eines übersehbaren Zeitraums die Tat begehen wird,

5. die Behörden der Zollverwaltung und die nach Landesrecht zuständigen Behörden zur Verhütung einer Straftat nach den §§ 10, 10a oder 11 des Schwarzarbeitsbekämpfungsgesetzes oder § 266a des Strafgesetzbuches,

6. die Verfassungsschutzbehörden des Bundes und der Länder, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach

   a) § 3 Absatz 1 des Bundesverfassungsschutzgesetzes, oder

   b) einem zum Verfassungsschutz (§ 1 Absatz 1 des Bundesverfassungsschutzgesetzes) landesgesetzlich begründeten Beobachtungsauftrag der Landesbehörde, insbesondere zum Schutz der verfassungsmäßigen Ordnung vor Bestrebungen und Tätigkeiten der organisierten Kriminalität,

7. den Militärischen Abschirmdienst, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach § 1 Absatz 1 des MAD-Gesetzes oder zur Sicherung der Einsatzbereitschaft der Truppe oder zum Schutz der Angehörigen, der Dienststellen und Einrichtungen des Geschäftsbereichs des Bundesministeriums der Verteidigung nach § 14 Absatz 1 des MAD-Gesetzes erforderlich ist,

8. den Bundesnachrichtendienst, soweit dies erforderlich ist

   a) zur politischen Unterrichtung der Bundesregierung, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Auskunft Informationen über das Ausland gewonnen werden können, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind und zu deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat, oder

   b) zur Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Auskunft Erkenntnisse gewonnen werden können mit Bezug zu den in § 4 Absatz 3 Nummer 1 des BND-Gesetzes genannten Gefahrenbereichen oder zum Schutz der in § 4 Absatz 3 Nummer 2 und 3 des BND-Gesetzes genannten Rechtsgüter.

(5) Derjenige, der geschäftsmäßig digitale Dienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Eine Verschlüsselung der Daten bleibt unberührt. Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(6) Wer geschäftsmäßig digitale Dienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. Jedes Auskunftsverlangen ist durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen

zu prüfen. Die weitere Bearbeitung des Auskunftsverlangens darf erst nach einem positiven Prüfergebnis freigegeben werden.

§ 23 Auskunftsverfahren bei Passwörtern und anderen Zugangsdaten

(1) Abweichend von § 22 darf derjenige, der geschäftsmäßig digitale Dienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, die als Bestandsdaten erhobenen Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 2 genannten Stellen verwenden. Für die Auskunftserteilung sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) Die Auskunft nach Absatz 1 Satz 1 darf nur erteilt werden an

1. zur Verfolgung von Straftaten zuständige Behörden, soweit diese im Einzelfall die Übermittlung unter Angabe einer gesetzlichen Bestimmung, die ihnen eine Erhebung und Nutzung der in Absatz 1 genannten Daten zur Verfolgung besonders schwerer Straftaten nach § 100b Absatz 2 Nummer 1 Buchstabe a, c, e, f, g, h oder m, Nummer 3 Buchstabe b erste Alternative, Nummer 5, 6, 9 oder 10 der Strafprozessordnung erlauben, nach Anordnung durch ein Gericht verlangen, oder
2. für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständige Behörden, soweit diese im Einzelfall die Übermittlung unter Angabe einer gesetzlichen Bestimmung, die ihnen eine Erhebung und Nutzung der in Absatz 1 genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit der Person, für die sexuelle Selbstbestimmung, für den Bestand des Bundes oder eines Landes, die freiheitlich demokratische Grundordnung sowie Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, erlauben, nach Anordnung durch ein Gericht verlangen.

An andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. Die Verantwortung für die Zulässigkeit der Auskunft tragen die um Auskunft ersuchenden Stellen.

(3) Derjenige, der geschäftsmäßig digitale Dienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Eine Verschlüsselung der Daten bleibt unberührt. Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(4) Wer geschäftsmäßig digitale Dienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. Jedes Auskunftsverlangen ist durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen zu prüfen. Die weitere Bearbeitung des Auskunftsverlangens darf erst nach einem positiven Prüfergebnis freigegeben werden.

§ 24 Auskunftsverfahren bei Nutzungsdaten

(1) Wer geschäftsmäßig digitale Dienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, darf die Nutzungsdaten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Für die Auskunftserteilung sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) Die Auskunft darf nur erteilt werden nach Maßgabe der nachfolgenden Absätze und soweit die um die Auskunft ersuchende Stelle dies im Einzelfall unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt. Das Auskunftsverlangen ist schriftlich oder elektronisch zu stellen. Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich schriftlich oder elektronisch zu bestätigen. Die Verantwortung für die Zulässigkeit der Auskunft tragen die um Auskunft ersuchenden Stellen.

(3) Die Auskunft nach Absatz 1 Satz 1 darf nur erteilt werden an

1. die für die Verfolgung von Straftaten zuständigen Behörden, soweit zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen und die zu erhebenden Daten erforderlich sind, um den Sachverhalt zu erforschen, den Aufenthaltsort eines Beschuldigten zu ermitteln,
2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden, soweit dies im Einzelfall erforderlich ist,

a) zur Abwehr einer Gefahr für

aa) die öffentliche Sicherheit, wobei die Auskunft auf Nutzungsdaten nach § 2 Absatz 2 Nummer 3 Buchstabe a beschränkt ist, oder

bb) Leib, Leben, Freiheit der Person, die sexuelle Selbstbestimmung, den Bestand und die Sicherheit des Bundes oder eines Landes, die freiheitlich demokratische Grundordnung, Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie nicht unerhebliche Sachwerte, oder

b) zum Schutz von Leib, Leben, Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung, Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie nicht unerheblichen Sachwerten, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes sowie zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder

c) zum Schutz von Leib, Leben Freiheit der Person, sexueller Selbstbestimmung, dem Bestand und der Sicherheit des Bundes oder eines Landes, der freiheitlich demokratischen Grundordnung sowie Gütern der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in einem übersehbaren Zeitraum eine gegen ein solches Rechtsgut gerichtete Straftat begehen wird, oder

d) zur Verhütung einer Straftat von erheblicher Bedeutung, sofern Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine ihrer Art nach konkretisierten Weise als Täter oder Teilnehmer an der Begehung einer Tat beteiligt ist, oder

e) zur Verhütung einer schweren Straftat nach § 100a Absatz 2 der Strafprozessordnung, sofern das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass die Person innerhalb eines übersehbaren Zeitraums die Tat begehen wird,

3. das Bundeskriminalamt als Zentralstelle nach § 2 des Bundeskriminalamtgesetzes, sofern im Einzelfall eine erhebliche Gefahr für die öffentliche Sicherheit vorliegt oder zureichende tatsächliche Anhaltspunkte für eine Straftat im Sinne des § 2 Absatz 1 des Bundeskriminalamtgesetzes vorliegen und die Daten erforderlich sind, um die zuständige Strafverfolgungsbehörde oder zuständige Polizeibehörde zu ermitteln, wobei die Auskunft auf Nutzungsdaten nach § 2 Absatz 2 Nummer 3 Buchstabe a beschränkt ist,

4. das Zollkriminalamt, soweit dies im Einzelfall erforderlich ist zum Schutz der in § 4 Absatz 1, auch in Verbindung mit Absatz 2, des Außenwirtschaftsgesetzes genannten Rechtsgüter, wenn

a) Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes sowie zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder

b) das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in einem übersehbaren Zeitraum eine gegen ein solches Rechtsgut gerichtete Straftat begehen wird,

5. die Verfassungsschutzbehörden des Bundes und der Länder, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach

a) § 3 Absatz 1 des Bundesverfassungsschutzgesetzes oder

b) einem zum Verfassungsschutz (§ 1 Absatz 1 des Bundesverfassungsschutzgesetzes) landesgesetzlich begründeten Beobachtungsauftrag der Landesbehörde, insbesondere zum Schutz der verfassungsmäßigen Ordnung vor Bestrebungen und Tätigkeiten der organisierten Kriminalität,

6. den Militärischen Abschirmdienst, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach § 1 Absatz 1 des MAD-Gesetzes oder zur Sicherung der Einsatzbereitschaft der Truppe oder zum Schutz der Angehörigen, der Dienststellen und Einrichtungen des Geschäftsbereichs des Bundesministeriums der Verteidigung nach § 14 Absatz 1 des MAD-Gesetzes erforderlich ist,

7. den Bundesnachrichtendienst zur Gewinnung von Erkenntnissen über das Ausland von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland, sofern

a) tatsächliche Anhaltspunkte dafür vorliegen, dass ein wenigstens seiner Art nach konkretisiertes sowie zeitlich absehbares Geschehen besteht, an dem bestimmte Personen beteiligt sein werden, und das

aa) einem der in § 4 Absatz 3 Nummer 1 des BND-Gesetzes genannten Gefahrenbereiche unterfällt, oder

bb) eines der in § 4 Absatz 3 Nummer 2 und 3 des BND-Gesetzes genannten Rechtsgüter beeinträchtigen wird, oder

b) eine Auskunftserteilung über bestimmte Nutzungsdaten im Sinne von § 2 Absatz 2 Nummer 3 Buchstabe a erforderlich ist, um einen Nutzer zu identifizieren, von dem ein bestimmter, dem Bundesnachrichtendienst bereits bekannter Inhalt der Nutzung des digitalen Dienstes herrührt, zum Zweck

aa) der politischen Unterrichtung der Bundesregierung, wenn im Einzelfall tatsächliche Anhaltspunkte für bestimmte Vorgänge im Ausland vorliegen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind und zu deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat, oder

bb) der Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung, wenn im Einzelfall tatsächliche Anhaltspunkte für Vorgänge im Ausland bestehen, die einen Bezug zu den in § 4 Absatz 3 Nummer 1 des BND-Gesetzes genannten Gefahrenbereichen aufweisen oder darauf abzielen oder geeignet sind, die in § 4 Absatz 3 Nummer 2 und 3 des BND-Gesetzes genannten Rechtsgüter zu schädigen.

(4) Derjenige, der geschäftsmäßig digitale Dienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Eine Verschlüsselung der Daten bleibt unberührt. Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(5) Wer geschäftsmäßig digitale Dienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. Jedes Auskunftsverlangen ist durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen zu prüfen. Die weitere Bearbeitung des Auskunftsverlangens darf erst nach einem positiven Prüfergebnis freigegeben werden.

Kapitel 2
Endeinrichtungen

§ 25 Schutz der Privatsphäre bei Endeinrichtungen

(1) Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 2016/679 zu erfolgen.

(2) Die Einwilligung nach Absatz 1 ist nicht erforderlich,

1. wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder
2. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines digitalen Dienstes einen vom Nutzer ausdrücklich gewünschten digitalen Dienst zur Verfügung stellen kann.

§ 26 Anerkannte Dienste zur Einwilligungsverwaltung, Endnutzereinstellungen

(1) Dienste zur Verwaltung von nach § 25 Absatz 1 erteilten Einwilligungen, die

1. nutzerfreundliche und wettbewerbskonforme Verfahren und technische Anwendungen zur Einholung und Verwaltung der Einwilligung haben,
2. kein wirtschaftliches Eigeninteresse an der Erteilung der Einwilligung und an den verwalteten Daten haben und unabhängig von Unternehmen sind, die ein solches Interesse haben können,
3. die personenbezogenen Daten und die Informationen über die Einwilligungsentscheidungen für keine anderen Zwecke als die Einwilligungsverwaltung verarbeiten und
4. ein Sicherheitskonzept vorlegen, das eine Bewertung der Qualität und Zuverlässigkeit des Dienstes und der technischen Anwendungen ermöglicht und aus dem sich ergibt, dass der Dienst sowohl technisch als auch organisatorisch die rechtlichen Anforderungen an den Datenschutz und die Datensicherheit, die sich insbesondere aus der Verordnung (EU) 2016/679 ergeben, erfüllt,

können von einer unabhängigen Stelle nach Maßgabe der Rechtsverordnung nach Absatz 2 anerkannt werden.

(2) Die Bundesregierung bestimmt durch Rechtsverordnung mit Zustimmung des Bundestages und des Bundesrates die Anforderungen

1. an das nutzerfreundliche und wettbewerbskonforme Verfahren und technische Anwendungen nach Absatz 1 Nummer 1 und
2. an das Verfahren der Anerkennung, insbesondere
   a) den erforderlichen Inhalt des Antrags auf Anerkennung,
   b) den Inhalt des Sicherheitskonzepts nach Absatz 1 Nummer 4 und
   c) die für die Anerkennung zuständige unabhängige Stelle, und
3. die technischen und organisatorischen Maßnahmen, dass
   a) Software zum Abrufen und Darstellen von Informationen aus dem Internet,
      aa) Einstellungen der Endnutzer hinsichtlich der Einwilligung nach § 25 Absatz 1 befolgt und
      bb) die Einbindung von anerkannten Diensten zur Einwilligungsverwaltung berücksichtigt und
   b) Anbieter von digitalen Diensten bei der Verwaltung der von Endnutzern erteilten Einwilligung die Einbindung von anerkannten Diensten zur Einwilligungsverwaltung und Einstellungen durch die Endnutzer berücksichtigen.

(3) Die Bundesregierung bewertet innerhalb von zwei Jahren nach Inkrafttreten einer Rechtsverordnung nach Absatz 1 die Wirksamkeit der getroffenen Maßnahmen im Hinblick auf die Errichtung nutzerfreundlicher und wettbewerbskonformer Einwilligungsverfahren und legt dazu einen Bericht an den Bundestag und den Bundesrat vor.

Teil 4
Straf- und Bußgeldvorschriften und Aufsicht

§ 27 Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. entgegen § 5 Absatz 1 eine Nachricht abhört oder in vergleichbarer Weise zur Kenntnis nimmt,
2. entgegen § 5 Absatz 2 Satz 1 eine Mitteilung macht oder
3. entgegen § 8 Absatz 1 eine dort genannte Telekommunikationsanlage herstellt oder auf dem Markt bereitstellt.

(2) Handelt der Täter in den Fällen des Absatzes 1 Nummer 3 fahrlässig, so ist die Strafe Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.

§ 28 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 8 Absatz 6 für eine Telekommunikationsanlage wirbt,

2. entgegen § 9 Absatz 1 Satz 1 oder Absatz 2 Satz 1 Verkehrsdaten verarbeitet,
3. entgegen § 10 Absatz 2 Satz 3 dort genannte Daten nicht oder nicht rechtzeitig löscht,
4. entgegen § 12 Absatz 1 Satz 3 Verkehrsdaten verarbeitet,
5. entgegen § 12 Absatz 2 Verkehrsdaten nicht oder nicht rechtzeitig löscht,
6. entgegen § 12 Absatz 3 Satz 2 eine dort genannte Aufzeichnung nicht oder nicht rechtzeitig löscht,
7. entgegen § 12 Absatz 4 Satz 5 oder § 14 Absatz 5 die Aufsichtsbehörde nicht oder nicht rechtzeitig in Kenntnis setzt,
8. entgegen § 13 Absatz 1 Satz 2 den Endnutzer nicht, nicht richtig oder nicht rechtzeitig informiert,
9. entgegen § 15 Absatz 2 erster Halbsatz die Rufnummernanzeige unterdrückt oder veranlasst, dass diese unterdrückt wird,
10. entgegen § 19 Absatz 1 nicht sicherstellt, dass der Nutzer einen dort genannten Dienst beenden oder in Anspruch nehmen kann,
11. entgegen § 20 personenbezogene Daten verarbeitet,
12. entgegen § 22 Absatz 5 Satz 1, § 23 Absatz 3 Satz 1 oder § 24 Absatz 4 Satz 1 die dort genannten Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt oder
13. entgegen § 25 Absatz 1 Satz 1 eine Information speichert oder auf eine Information zugreift.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2, 3, 9, 11, 12 und 13 mit einer Geldbuße bis zu dreihunderttausend Euro, in den Fällen des Absatzes 1 Nummer 4 und 5 mit einer Geldbuße bis zu hunderttausend Euro, in den Fällen des Absatzes 1 Nummer 8 mit einer Geldbuße bis zu fünfzigtausend Euro und in den übrigen Fällen mit einer Geldbuße bis zu zehntausend Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist

1. die Bundesnetzagentur in den Fällen des Absatzes 1 Nummer 1 und 9,
2. der Bundesbeauftragte oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in den Fällen des Absatzes 1 Nummer 2 bis 8 und im Fall des Absatzes 1 Nummer 13, soweit die Speicherung von oder der Zugriff auf Informationen durch Anbieter von Telekommunikationsdiensten oder durch Bundesbehörden erfolgt.

(4) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 oder Absatz 2 des Bundesdatenschutzgesetzes werden keine Geldbußen verhängt.

§ 29 Zuständigkeit, Aufgaben und Befugnisse der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen verarbeitet werden, ist der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die zuständige Aufsichtsbehörde.

(2) Erfolgt die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, durch Anbieter von Telekommunikationsdiensten oder durch öffentliche Stellen des Bundes, ist der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständige Aufsichtsbehörde für die Einhaltung des § 25.

(3) Im Hinblick auf die Befugnisse des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen seiner oder ihrer Aufsichtstätigkeit über die Einhaltung der Bestimmungen nach diesem Gesetz findet Artikel 58 der Verordnung (EU) 2016/679 entsprechende Anwendung.

(4) Das Fernmeldegeheimnis des Artikels 10 des Grundgesetzes wird eingeschränkt, soweit die Wahrnehmung der Befugnisse nach Absatz 3 dies erfordert.

§ 30 Zuständigkeit, Aufgaben und Befugnisse der Bundesnetzagentur

(1) Die Bundesnetzagentur ist zuständige Aufsichtsbehörde für die Einhaltung der Vorschriften in Teil 2, soweit nicht gemäß § 29 die Zuständigkeit des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gegeben ist.

(2) Die Bundesnetzagentur kann Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Vorschriften des Teils 2 sicherzustellen. Der nach den Vorschriften des Teils 2 Verpflichtete muss auf Anforderung der Bundesnetzagentur die hierzu erforderlichen Auskünfte erteilen. Die Bundesnetzagentur ist zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten zu betreten und zu besichtigen.

(3) Über die Befugnis zu Anordnungen nach Absatz 2 hinaus kann die Bundesnetzagentur bei Nichterfüllung von Verpflichtungen des Teils 2 den Betrieb von betroffenen Telekommunikationsanlagen oder das Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen.

(4) Zur Durchsetzung von Maßnahmen und Anordnungen nach den Absätzen 2 und 3 kann nach Maßgabe des Verwaltungsvollstreckungsgesetzes ein Zwangsgeld bis zu 1 Million Euro festgesetzt werden.

(5) Das Fernmeldegeheimnis des Artikels 10 des Grundgesetzes wird eingeschränkt, soweit die Wahrnehmung der Befugnisse nach Absatz 2 Satz 1 und 3 dies erfordert.